特許協力条約に基づいて公開された国際出願

10/049264

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002年5月16日 (16.05.2002)

PCT

(10) 国際公開番号
WO 02/39664 A2

(51) 国際特許分類[7]: H04L 9/30, G09C 1/00

(21) 国際出願番号: PCT/JP01/09781

(22) 国際出願日: 2001年11月8日 (08.11.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-345457 2000年11月8日 (08.11.2000) JP
特願2000-393279 2000年12月21日 (21.12.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 桶屋勝幸 (OKEYA, Katsuyuki) [JP/JP]; 〒244-0003 神奈川県横浜市戸塚区戸塚町5030番地 株式会社 日立製作所 ソフトウェア事業部内 Kanagawa (JP).

(74) 代理人: 浅村 皓, 外(ASAMURA, Kiyoshi et al.); 〒100-0004 東京都千代田区大手町2丁目2番1号 新大手町ビル331 Tokyo (JP).

(81) 指定国 (国内): US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 第17条(2)(a)に基づく宣言；要約なし；国際調査機関により点検されていない発明の名称。

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

WO 02/39664 A2

(54) Title: ELLIPTIC CURVE SCALAR MULTIPLE CALCULATION METHOD AND DEVICE, AND STORAGE MEDIUM

(54) 発明の名称: 楕円曲線スカラー倍計算方法及び装置並びに記憶媒体

(57) Abstract:

# 明　細　書

## 楕円曲線スカラー倍計算方法及び装置並びに記憶媒体

### 技術分野

本発明はコンピュータネットワークにおけるセキュリティ技術に係り、特に楕円曲線暗号における暗号処理実行方法に関する。

### 背景技術

楕円曲線暗号はN. Koblitz, V. S. Millerにより提案された公開鍵暗号の一種である。公開鍵暗号には、公開鍵と呼ばれる一般に公開してよい情報と、秘密鍵と呼ばれる秘匿しなければならない秘密情報がある。与えられたメッセージの暗号化や署名の検証には公開鍵を用い、与えられたメッセージの復号化や署名の作成には秘密鍵を用いる。楕円曲線暗号における秘密鍵は、スカラー値が担っている。また、楕円曲線暗号の安全性は楕円曲線上の離散対数問題の求解が困難であることに由来している。ここで楕円曲線上の離散対数問題とは、楕円曲線上のある点Pとそのスカラー倍の点dPが与えられた時、スカラー値dを求める問題である。ここにおいて、楕円曲線上の点とは、楕円曲線の定義方程式をみたす数の組をいい、楕円曲線上の点全体には、無限遠点という仮想的な点を単位元とした演算、すなわち楕円曲線上の加法（乃至は加算）が定義される。そして、同じ点同士の楕円曲線上の加法のことを、特に楕円曲線上の２倍算という。楕円曲線上の２点の加法は次のようにして計算される。２点を通る直線を引くとその直線は楕円曲線と他の点において交わる。その交わった点とｘ軸に関して対称な点を加法を行なった結果の点とする。楕円曲線上の点の２倍算は次のようにして計算される。楕円曲線上の点における接線をひくと、その接線は楕円曲線上の他の点において交わる。その交わった点とｘ座標に関して対称な点を２倍算を行なった結果の点とする。ある点に対し、特定の回数だけ加法を行なうことをスカラー倍といい、その結果をスカラー倍点、その回数のことをスカラー値という。

情報通信ネットワークの進展と共に電子情報に対する秘匿や認証の為に暗号技術は不可欠な要素となってきている。そこでは暗号技術の安全性とともに高速化

が望まれている。楕円曲線上の離散対数問題が非常に困難である為に、素因数分解の困難性を安全性の根拠にしているＲＳＡ暗号と比べて、楕円曲線暗号は鍵長を比較的短くすることができる。そのため比較的高速な暗号処理が可能である。しかしながら、処理能力の制限されているスマートカードや大量の暗号処理を行なう必要のあるサーバ等においては、必ずしも満足できる程高速であるとは限らない。それゆえに暗号のさらなる高速化が必要となる。

楕円曲線暗号には、ワイエルシュトラス型楕円曲線と呼ばれる楕円曲線が通常用いられている。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology roceedings of ASIACRYPT'98, LNCS 1514, Springer-Verlag, (1998) pp. 51-65には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この計算方法は、スカラー倍点の座標を、省略することなく正確に表示している。すなわち、アフィン座標系であれば、ｘ座標及びｙ座標、射影座標乃至はヤコビアン座標であれば、Ｘ座標、Ｙ座標及びＺ座標の値を全て与えている。

一方でモンゴメリ型楕円曲線$BY^2=X^3+AX^2+X$（$A, B\in F_p$）を用いるとワイエルシュトラス型楕円曲線よりも高速に演算を実行できることがP. L. Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization, Math. Comp. 48 (1987) pp. 243-264. に記載されている。これは、スカラー値の特定のビットの値に依存して、楕円曲線上の点の組(mP, (m+1)P)から点の組(2mP, (2m+1)P)乃至は点の組((2m+1)P, (2m+2)P)を繰り返し計算するスカラー倍計算方法において、モンゴメリ型楕円曲線を利用することにより、加算及び２倍算の計算時間が短縮されることに由来する。このスカラー倍計算法は、ワイエルシュトラス型楕円曲線における、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いた場合よりも、高速に計算することができる。しかしながら、この方法は楕円曲線上の点のｙ座標の値は計算しない。多くの暗号処理においては、本質的にy座標を用いないので、この事は問題にはならないが、一部の暗号処理を実行する又は完全な形で標準に準拠しようとすれ

ば、y座標の値も必要となる。

以上は楕円曲線の定義体の標数が５以上の素数の場合であるが、他方、標数２の有限体上定義された楕円曲線に対しては、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法が J. Lopez, R. Dahab, Fast Multiplication on Elliptic Curves over GF($2^m$) without Precomputation, Cryptographics Hardware and Embedded Systems: Proceedings of CHES'99, LNCS 1717, Springer-Verlag, (1999) pp. 316-327. に記載されている。

上記従来技術により、標数が５以上の有限体上定義された楕円曲線を用いて楕円曲線暗号を構成した場合、ワイエルシュトラス型楕円曲線においてウィンドウ法及び混合座標系を用いると、スカラー倍点の座標を完全に計算することができるが、モンゴメリ型楕円曲線のスカラー倍計算方法を用いた場合程高速に計算することはできない。モンゴメリ型楕円曲線におけるスカラー倍計算方法を用いると、ワイエルシュトラス型楕円曲線においてウィンドウ法及び混合座標系を用いた場合より高速に計算することが可能であるが、スカラー倍点の座標を完全に与えること、すなわちｙ座標を計算することができない。したがって、スカラー倍計算方法として、高速化を計ろうとするとスカラー倍点の座標を完全に与えることができず、スカラー倍点の座標を完全に与えようとすると高速に計算ができないという状態にあった。

発明の開示

本発明の目的は、標数が５以上の有限体上定義された楕円曲線において、モンゴメリ型楕円曲線におけるスカラー倍演算と同程度の高速さで、スカラー倍点の座標を完全に与えることができる、即ち、ｘ座標とｙ座標を共に計算できるスカラー倍計算方法を提供することにある。

上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限

体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報からアフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から射影座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のＸ座標及びＺ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるＸ座標及びＺ座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のＸ座標及びＺ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるＸ座標及びＺ座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のＸ座標及びＺ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるＸ座標及びＺ座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点のｘ座標、前記スカラー倍点と前

記モンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるx座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点のx座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点のアフィ

ン座標におけるx座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、アフィン座標において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からワイエルシュトラス型楕円曲線において完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からモンゴメリ型楕円曲線において完全な座標を復元するステップと、前記モンゴメリ型楕円曲線において完全な座標が復元されたスカラー倍点からワイエルシュトラス型楕円曲線におけるスカラー倍点を計算するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の

射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを含むことを特徴とする。

また本発明は、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴ

メリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有することを特徴とする。

また上記目的を達する一手段として、楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線においてアフィン座標で与えられたスカラー倍点のx座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるx座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有することを特徴とする。

図面の簡単な説明

図1は本発明の暗号処理システムの構成図である。

図2は本発明の実施例におけるスカラー倍計算方法及び装置における処理の流れを示す図である。

図3は図1の暗号処理システムでの処理の流れを示すシーケンス図である。

図4は本発明の第1、第2、第14及び第15実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図5は本発明の第3及び第4実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図６は本発明の第５実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図７は本発明の第６、第７及び第８実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図８は本発明の第９、第１０、第２０及び第２１実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図９は本発明の第２実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１０は本発明の第１１及び第１２実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図１１は本発明の第１実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１２は本発明の第３実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１３は本発明の第４実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１４は本発明の第６実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１５は本発明の第７実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１６は本発明の第８実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１７は本発明の第９実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１８は本発明の第１０実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図１９は本発明の第１１実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図２０は本発明の第１２実施例のスカラー倍計算方法における座標復元方法を

示すフローチャート図である。

図２１は本発明の第１３実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図２２は本発明の実施の形態に係る署名作成装置の構成図である。

図２３は本発明の実施の形態に係る復号化装置の構成図である。

図２４は本発明の第１３実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図２５は図２のスカラー倍計算部におけるスカラー倍計算方法を示すフローチャートである。

図２６は本発明の第５実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図２７は本発明の実施例におけるスカラー倍計算方法及び装置における処理の流れを示す図である。

図２８は図２２の署名作成装置における署名作成方法を示すフローチャートである。

図２９は図２２の署名作成装置における処理の流れを示すシーケンス図である。

図３０は図２３の復号化装置における復号化方法を示すフローチャートである。

図３１は図２３の復号化装置における処理の流れを示すシーケンス図である。

図３２は図１の暗号処理システムにおける暗号処理方法を示すフローチャートである。

図３３は図２７のスカラー倍計算部におけるスカラー倍計算方法を示すフローチャートである。

図３４は本発明の第１４実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図３５は本発明の第１５実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図３６は本発明の第１６実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図３７は本発明の第１７実施例のスカラー倍計算方法における座標復元方法を

示すフローチャート図である。

図３８は本発明の第１８実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図３９は本発明の第１９実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図４０は本発明の第２０実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図４１は本発明の第２１実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図４２は本発明の第２２実施例のスカラー倍計算方法における座標復元方法を示すフローチャート図である。

図４３は本発明の第１６実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図４４は本発明の第１７、第１８及び第１９実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

図４５は本発明の第２２実施例のスカラー倍計算方法における高速スカラー倍計算方法を示すフローチャート図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面により説明する。

図１は暗号/復号処理装置の構成を示したものである。この暗号/復号処理装置１０１は、入力されたメッセージの暗号化、暗号化されたメッセージの復号化のいずれも行えるようにしたものである。尚、ここで扱う楕円曲線は標数５以上の楕円曲線とする。

入力されたメッセージを暗号化し、暗号化されたメッセージを復号化する場合、一般に次の数１が成立する。

$$Pm+k(aQ)-a(kQ)=Pm \qquad \cdots 数1$$

ここで、$P_m$はメッセージであり、ｋは乱数、ａは秘密鍵を示す定数、Ｑは定点である。この式のＰｍ＋ｋ（ａＱ）のａＱは、公開鍵を示しており、入力されたメッセージを公開鍵によって暗号化することを示している。ａ（ｋＱ）のａは

秘密鍵を示しており、秘密鍵により復号化することを示している。

従って、図１に示した暗号/復号処理装置１０１をメッセージの暗号化だけに用いる場合には、Ｐm＋ｋ（ａＱ）及びｋＱを計算して出力し、復号化だけに用いる場合には、秘密鍵ａ及びｋＱより－ａ（ｋＱ）を計算し、（Ｐm＋ｋ（ａＱ））－ａ（ｋＱ）を計算して出力するようにすればよい。

図１に示した暗号/復号処理装置１０１は、処理部１１０と、記憶部１２０、レジスタ部１３０とを有している。処理部１２０は、暗号化処理に必要な処理を機能ブロックで示しており、入力されたメッセージの暗号化や暗号化されたメッセージの復号化を行う暗号/復号処理部１０２、暗号/復号処理部１０２で暗号化や復号化を行うのに必要なパラメータを演算するスカラー倍計算部１０３とを有している。記憶部１２０は、定数、秘密情報（例えば、秘密鍵である。）などを記憶している。レジスタ部１３０は、暗号化又は復号化処理において演算の結果や、記憶部１２０に記憶された情報を一次的に記憶する。尚、処理部１１０、レジスタ部１３０は以下に説明する処理を行う専用の演算装置やＣＰＵなどにより実現することができ、記憶部１２０は、ＲＡＭ、ＲＯＭなどによって実現することができる。

次に、図１に示した暗号/復号処理装置１０１の動作について説明する。図３は、暗号/復号処理装置１０１において暗号化、復号化を行う場合の各部の情報の伝達を示したものである。

暗号／復号処理部１０２は暗号化処理を行なう場合は暗号化処理部１０２と表記し、復号化処理を行なう場合は復号化処理部１０２と表記する。

まず、図３０により入力されたメッセージを暗号化する場合の動作について説明する。

暗号／復号処理部１０２へメッセージが入力されると（３００１）、入力されたメッセージのビット長が予め定めたビット長か否かを判断する。予め定めたビット長より長い場合には、予め定めたビット長となるようにメッセージを区切る（以下、メッセージは所定のビット長に区切られているものとして説明する。）。次に、暗号/復号処理部１０２は、メッセージのビット列によって表される数値をｘ座標（ｘ1）にもつ楕円曲線上のｙ座標の値（ｙ1）を計算する。例えば、モ

ンゴメリ型楕円曲線は、$By1^2=x1^3+Ax1^2+x1$で表されるので、これよりｙ座標の値を求めることができる。尚、Ｂ、Ａはそれぞれ定数である。暗号化処理部１０２は、公開鍵ａＱ及びＱのｘ座標、ｙ座標の値をスカラー倍計算部１０３へ送る。このとき、暗号化処理部１０２は乱数を生成し、これをスカラー倍計算部１０３へ送る（３００２）。スカラー倍計算部１０３は、Ｑのｘ座標、ｙ座標の値、乱数によるスカラー倍点（ｘd1、ｙd1）と、公開鍵ａＱのｘ座標、ｙ座標の値、乱数によるスカラー倍点（ｘd2、ｙd2）とを計算し（３００３）、計算されたスカラー倍点を暗号化処理部１０２へ送る（３００４）。暗号化処理部１０２は、送られたスカラー倍点を用いて、暗号化処理を行う（３００５）。例えば、モンゴメリ型の楕円曲線については、次式により暗号化されたメッセージｘe1、ｘe2を得る。

$$xe1=B\left((yd1-y1)/(xd1-x1)\right)^2-A-x1-xd1 \quad \cdots数２$$

$$xe2=xd2 \quad \cdots数３$$

暗号/復号処理装置１０１は暗号/復号処理部１０２で暗号化されたメッセージを出力する。

次に、図３２により暗号化されたメッセージを復号化する場合の動作について説明する。

暗号／復号処理部１０２へ暗号化されたメッセージが入力されると（３２０１）、暗号化されたメッセージのビット列によって表される数値をｘ座標にもつ楕円曲線上のｙ座標の値を計算する。ここで、暗号化されたメッセージがｘe1、ｘe2のビット列であり、モンゴメリ型楕円曲線の場合、ｙ座標の値（ｙe1）は$Bye1^2=xe1^3+Axe1^2+xe1$から得られる。尚、Ｂ、Ａはそれぞれ定数である。暗号／復号処理部１０２は、ｘ座標、ｙ座標の値（ｘe1、ｙe1）をスカラー倍計算部１０３へ送る（３２０２）。スカラー倍計算部１０３は記憶部１２０から秘密情報を読み出し（３２０３）、ｘ座標、ｙ座標の値、秘密情報からスカラー倍点（ｘd3、ｙd3）を計算し（３２０４）、計算されたスカラー倍点を暗号/復号処理部１０２へ送る（３２０５）。暗号／復号処理部１０２は、送られたスカラー倍点を用いて、復号化処理を行う（３２０６）。例えば、暗号化されたメッセージが、ｘe1、ｘe2のビット列であり、モンゴメリ型の楕円曲線の場合は、

次式によりｘｆ1を得る。

$xf1=B((ye2+yd3)/(xe2-xd3))^2-A-xe2-xd3$ …数４

このｘｆ1は、暗号化される前のメッセージｘ１に相当するものである。

復号処理部１０２は復号化されたメッセージxf1を出力する（３２０７）

以上のようにして、暗号/復号処理部１０２により暗号化、または復号化処理が行われる。

次に、暗号化処理装置１０１のスカラー倍計算部１０３の処理について説明する。ここでは、暗号化処理装置１０１が、復号化処理を行う場合を例に以下、説明する。

図２は、スカラー倍計算部１０３の機能ブロックを示したものである。図２５は、スカラー倍計算部１０３の動作を示したものである。

高速スカラー倍計算部２０２が、秘密情報であるスカラー値及び暗号化されたメッセージと、暗号化されたメッセージがX座標となる楕円曲線上のY座標の値である楕円曲線上の点を受け取る（ステップ２５０１）と、高速スカラー倍計算部２０２は受け取ったスカラー値と楕円曲線上の点からスカラー倍点の座標の一部の値を計算し（ステップ２５０２）、その情報を座標復元部２０３に与える（ステップ２５０３）。座標復元部２０３は与えられたスカラー倍点の情報及び入力された楕円曲線上の点よりスカラー倍点の座標の復元を行なう（ステップ２５０４）。スカラー倍計算部１０３は完全に座標が与えられたスカラー倍点を計算結果として出力する（ステップ２５０５）。ここで、完全に座標が与えられたスカラー倍点とは、y座標が計算されて出力されることを意味する（以下、同じ。）。

以下、スカラー倍計算部１０３の高速スカラー倍計算部２０２、座標復元部２０３についていくつかの実施例を説明する。

第１の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Ｐから、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点（$x_d$，$y_d$）を計算し出力するものである。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値ｄと与えられたモンゴメリ型楕円曲線上の点Ｐから

モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点P＝(x, y)と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、x及びyよりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図１１により、座標x, y, $X_d$, $Z_d$, $X_{d+1}$, $Z_{d+1}$が与えられた場合に$x_d$, $y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d−1)Pのアフィン座標を$(x_{d-1}, y_{d-1})$で、射影座標を$(X_{d-1}, Y_{d-1}, Z_{d-1})$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ１１０１において$X_d \times x$が計算され、レジスタ$T_1$に格納される。ステップ１１０２において$T_1 - Z_d$が計算される。ここでレジスタ$T_1$には$X_d x$が格納されており、したがって$X_d x - Z_d$ が計算される。その結果がレジスタ$T_1$に格納される。ステップ１１０３において$Z_d \times x$が計算され、レジスタ$T_2$に格納される。ステップ１１０４において$X_d - T_2$が計算される。ここでレジスタ$T_2$

には$Z_d x$が格納されており、したがって$X_d-xZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１０５において$X_{d+1}\times T_2$が計算される。ここでレジスタＴ$_2$には$X_d-xZ_d$が格納されており、したがって$X_{d+1}(X_d-xZ_d)$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ１１０６においてＴ$_2$の２乗が計算される。ここでレジスタＴ$_2$には$(X_d-xZ_d)$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１０７において$T_2\times X_{d+1}$が計算される。ここでレジスタＴ$_2$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１０８において$T_2\times Z_{d+1}$が計算される。ここでレジスタＴ$_2$には$X_{d+1}(X_d-xZ_d)^2$が格納されており、したがって$Z_{d+1}X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１０９において$T_2\times y$が計算される。ここでレジスタＴ$_2$には$Z_{d+1}X_{d+1}(X_d-xZ_d)^2$が格納されており、したがって$yZ_{d+1}X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１１０において$T_2\times B$が計算される。ここでレジスタＴ$_2$には$yZ_{d+1}X_{d+1}(X_d-xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１１１において$T_2\times Z_d$が計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１１２において$T_2\times X_d$が計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d$が格納されており、したがって$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d$が計算される。その結果がレジスタＴ$_4$に格納される。ステップ１１１３において$T_2\times Z_d$が計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d$が格納されており、したがって$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１１４においてレジスタＴ$_2$の逆元が計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d{}^2$が格納されており、したがって$1/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d{}^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１１１５において$T_2\times T_4$が計算される。ここでレジスタ

$T_2$には$1/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$がレジスタ$T_4$には$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d$がそれぞれ格納されており、したがって$(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d)/(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2)(=X_d/Z_d)$が計算される。その結果がレジスタ$x_d$に格納される。ステップ１１１６において$T_1 \times Z_{d+1}$が計算される。ここでレジスタ$T_1$には$X_dx-Z_d$が格納されており、したがって$Z_{d+1}(X_dx-Z_d)$が計算される。その結果がレジスタ$T_4$に格納される。ステップ１１１７においてレジスタ$T_1$の２乗が計算される。ここでレジスタ$T_1$には$(X_dx-Z_d)$が格納されており、したがって$(X_dx-Z_d)^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１１１８において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(X_dx-Z_d)^2$がレジスタ$T_2$には$1/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$(X_dx-Z_d)^2/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$ が計算される。その結果がレジスタ$T_2$に格納される。ステップ１１１９において$T_3+T_4$が計算される。ここでレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)$ がレジスタ$T_4$には$Z_{d+1}$ $(X_dx-Z_d)$がそれぞれ格納されており、したがって$X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１１２０において$T_3-T_4$が計算される。ここでレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)$がレジスタ$T_4$には$Z_{d+1}(X_dx-Z_d)$がそれぞれ格納されており、したがって$X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)$が計算される。その結果がレジスタ$T_3$に格納される。ステップ１１２１において$T_1 \times T_3$が計算される。ここでレジスタ$T_1$には$X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)$がレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)$がそれぞれ格納されており、したがって$\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１１２２において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}$がレジスタ$T_2$には$(X_dx-Z_d)^2/ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$がそれぞれ格納されており、したがって

$$\frac{\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}(X_dx-Z_d)^2}{ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2}$$

… 数５

が計算される。その結果が$y_d$に格納される。$x_d$にはステップ１１１５において$(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2\ Z_dX_d)/(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2\ X_d^2)$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により座標復元部２０３へ与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からモンゴメリ型楕円曲線におけるスカラー倍点のアフィン座標($x_d$, $y_d$)における値が全て復元される理由は以下の通りである。尚、点(d+1)Pは点dPに点Pを加算した点であり、点(d−1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の式を得る。

$(A+x+x_d+x_{d+1})(x_d-x)^2=B(y_d-y)^2$ … 数６

$(A+x+x_d+x_{d-1})(x_d-x)^2=B(y_d+y)^2$ … 数７

両辺を各々減算することにより、

$(x_{d-1}-x_{d+1})(x_d-x)^2=4By_dy$ … 数８

を得る。したがって、

$y_d=(x_{d-1}-x_{d+1})(x_d-x)^2/4By$ … 数９

となる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$y_d=(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2/4ByZ_{d-1}Z_{d+1}Z_d^2$ … 数１０

モンゴメリ型楕円曲線の射影座標での加算公式は

$X_{m+n}=Z_{m-n}[(X_m-Z_m)(X_n+Z_n)+(X_m+Z_m)(X_n-Z_n)]^2$ … 数１１

$Z_{m+n}=X_{m-n}[(X_m-Z_m)(X_n+Z_n)-(X_m+Z_m)(X_n-Z_n)]^2$ … 数１２

である。ここで$X_m$及び$Z_m$はモンゴメリ型楕円曲線上の点Pのｍ倍点mPの射影座標におけるX座標及びZ座標、$X_n$及び$Z_n$はモンゴメリ型楕円曲線上の点Pのｎ倍点nPの射影座標におけるX座標及びZ座標、$X_{m-n}$及び$Z_{m-n}$はモンゴメリ型楕円曲線上の点Pの(m−n)倍点(m−n)Pの射影座標におけるX座標及びZ座標、$X_{m+n}$及び$Z_{m+n}$はモンゴメリ型楕円曲線上の点Pの(m+n)倍点(m+n)Pの射影座標におけるX座標及びZ座標であり、ｍ，ｎはｍ＞ｎをみたす正整数である。この式は$X_m/Z_m=x_m$、$X_n/Z_n=x_n$、$X_{m-n}/Z_{m-n}=x_{m-n}$が不変のとき、$X_{m+n}/Z_{m+n}$

$=x_{m+n}$も不変となるので、射影座標での公式としてうまく働いている。他方、

$$X'_{m-n}=Z_{m+n}\left[(X_m-Z_m)(X_n+Z_n)+(X_m+Z_m)(X_n-Z_n)\right]^2 \quad \cdots 数１３$$

$$Z'_{m-n}=X_{m+n}\left[(X_m-Z_m)(X_n+Z_n)-(X_m+Z_m)(X_n-Z_n)\right]^2 \quad \cdots 数１４$$

とおくと、この式で$X_m/Z_m=x_m$、$X_n/Z_n=x_n$、$X_{m+n}/Z_{m+n}=x_{m+n}$が不変のとき、$X'_{m-n}/Z'_{m-n}$も不変となる。また、$X'_{m-n}/Z'_{m-n}=X_{m-n}/Z_{m-n}$をみたすので、$x_{m-n}$の射影座標として$X'_{m-n}, Z'_{m-n}$をとってよい。$m=d$、$n=1$として上記公式を用いて$y_d$の式より$X_{d-1}$及び$Z_{d-1}$を消去し、$X_1=x, Z_1=1$とおくことにより、次の式を得る。

$$y_d=\frac{\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2}{ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2} \quad \cdots 数１５$$

$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、

$$x_d=\frac{ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d}{ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d} \quad \cdots 数１６$$

となる。ここで、$x_d$, $y_d$は図１１の処理により与えられている。したがって、アフィン座標$(x_d, y_d)$の値が全て復元されていることになる。

上記手順はステップ１１０１、ステップ１１０３、ステップ１１０５、ステップ１１０７、ステップ１１０８、ステップ１１０９、ステップ１１１０、ステップ１１１１、ステップ１１１２、ステップ１１１３、ステップ１１１５、ステップ１１１６、ステップ１１１８、ステップ１１２１及びステップ１１２２において有限体上の乗算の計算量を必要とする。また、ステップ１１０６及びステップ１１１７において有限体上の２乗算の計算量を必要とする。また、ステップ１１１４において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１５Ｍ＋２Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計

算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M、Ｉ＝４０Mと仮定すると座標復元の計算量は５６．６Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$，$y_d$の値が計算できれば$x_d$，$y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメータであるBの値を小さくとることにより、ステップ１１１０における乗算の計算量を削減することができる。

次に図４により、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力する高速スカラー倍計算部の処理を説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝($X_d$，$Y_d$，$Z_d$)のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝($X_{d+1}$，$Y_{d+1}$，$Z_{d+1}$)のうち$X_{d+1}$及び$Z_{d+1}$を出力する。ステップ４０１として、変数Ｉに初期値１を代入する。ステップ４０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(x，y，1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ４０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ４０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ４０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ４１３へ行く。一致しなければステップ４０５へ行く。ステップ４０５として、変数Ｉを１増加させる。ステップ４０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ４０７へ行く。そのビットの値が１であればステップ４１０へ行く。ステップ４０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算す

る。その後ステップ４０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ４０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４０９として、ステップ４０８で求めた点2mPとステップ４０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ４０４へ戻る。ここで、点２mP、点(２m+1)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ４１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ４１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ４１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４１２として、ステップ４１０で求めた点(2m+１)Pとステップ４１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ４０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ４１３として、射影座標で表された点の組(mP, (m+１)P)から、射影座標で表された点mP＝$(X_m, Y_m, Z_m)$より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$として、射影座標で表された点(m+1)P＝$(X_{m+1}, Y_{m+1}, Z_{m+1})$より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$として、出力する。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。また上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1$＝１ととることにより３Ｍ＋２Ｓとなる。ここでMは有限体上の乗算の計算量、Ｓは有限

体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ４０７において加算の計算量、ステップ４０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ４１０において加算の計算量、ステップ４１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ４０４、ステップ４０５、ステップ４０６、ステップ４０７、ステップ４０８、ステップ４０９乃至はステップ４０４、ステップ４０５、ステップ４０６、ステップ４１０、ステップ４１１、ステップ４１２の繰り返しの回数は、（スカラー値dのビット長）—１回となるので、ステップ４０２での２倍算の計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）（ｋ—１）＋３Ｍ＋２Ｓとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ—４．６）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１４６７Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A.Miyaji, T.Ono, H.Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp.51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６００Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Y_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用

いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１５Ｍ＋２Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ—４．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５２）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１５２４Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第２の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算し出力するものである。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたモンゴメリ型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点P＝(x, y)と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、x及びyよりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標$X_d, Y_d$及び$Z_d$の復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算結果として出力する。

次に図９により、座標x、y $X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$が与えられた場合に$X_d$、

$Y_d$、$Z_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝($X_d$, $Y_d$, $Z_d$)の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順で射影座標おいて完全な座標が与えられたスカラー倍点($X_d$, $Y_d$, $Z_d$)を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を($X_1$, $Y_1$, $Z_1$)でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を($x_d$, $y_d$)で、射影座標を($X_d$, $Y_d$, $Z_d$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d-1)Pのアフィン座標を($x_{d-1}$, $y_{d-1}$)で、射影座標を($X_{d-1}$, $Y_{d-1}$, $Z_{d-1}$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を($x_{d+1}$, $y_{d+1}$)で、射影座標を($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)でそれぞれ表す。

ステップ９０１において$X_d \times x$が計算され、レジスタＴ$_1$に格納される。ステップ９０２においてＴ$_1$－$Z_d$が計算される。ここでレジスタＴ$_1$には$X_d x$が格納されており、したがって$X_d x - Z_d$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ９０３において$Z_d \times x$が計算され、レジスタＴ$_2$に格納される。ステップ９０４において$X_d$－Ｔ$_2$が計算される。ここでレジスタＴ$_2$には$Z_d x$が格納されており、したがって$X_d - xZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ９０５において$Z_{d+1} \times$Ｔ$_1$が計算される。ここでレジスタＴ$_1$には$X_d x - Z_d$が格納されており、したがって$Z_{d+1}(X_d x - Z_d)$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ９０６において$X_{d+1} \times$Ｔ$_2$が計算される。ここでレジスタＴ$_2$には$X_d - xZ_d$が格納されており、したがって$X_{d+1}(X_d - xZ_d)$が計算される。その結果がレジスタＴ$_4$に格納される。ステップ９０７においてＴ$_1$の２乗が計算される。ここでレジスタＴ$_1$には$X_d x - Z_d$が格納されており、したがって$(X_d x - Z_d)^2$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ９０８においてＴ$_2$の２乗が計算される。ここでレジスタＴ$_2$には$X_d - xZ_d$が格納されており、したがって$(X_d - xZ_d)^2$が計算

される。その結果がレジスタ$T_2$に格納される。ステップ９０９において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$(X_d - xZ_d)^2$が格納されており、したがって$Z_d(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ９１０において$T_2 \times X_{d+1}$が計算される。ここでレジスタ$T_2$には$Z_d(X_d - xZ_d)^2$が格納されており、したがって$X_{d+1}Z_d(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ９１１において$T_2 \times Z_{d+1}$が計算される。ここでレジスタ$T_2$に$X_{d+1}Z_d(X_d - xZ_d)^2$が格納されており、したがって$Z_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ９１２において$T_2 \times y$が計算される。ここでレジスタ$T_2$には$Z_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が格納されており、したがって$yZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ９１３において$T_2 \times B$が計算される。ここでレジスタ$T_2$には$yZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ９１４において$T_2 \times X_d$が計算される。ここでレジスタ$T_2$には$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2X_d$が計算される。その結果が$X_d$に格納される。ステップ９１５において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2Z_d$が計算される。その結果がレジスタ$Z_d$に格納される。ステップ９１６において$T_3 + T_4$が計算される。ここでレジスタ$T_3$には$Z_{d+1}(X_dx - Z_d)$がレジスタ$T_4$には$X_{d+1}(X_d - xZ_d)$が格納されており、したがって$Z_{d+1}(X_dx - Z_d) + X_{d+1}(X_d - xZ_d)$が計算される。その結果がレジスタ$T_2$に格納される。ステップ９１７において$T_3 - T_4$が計算される。ここでレジスタ$T_3$には$Z_{d+1}(X_dx - Z_d)$がレジスタ$T_4$には$X_{d+1}(X_d - xZ_d)$が格納されており、したがって$Z_{d+1}(X_dx - Z_d) - X_{d+1}(X_d - xZ_d)$が計算される。その結果がレジスタ$T_3$に格納される。ステップ９１８において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(X_dx - Z_d)^2$がレジスタ$T_2$には$Z_{d+1}(X_dx - Z_d) + X_{d+1}(X_d - xZ_d)$が格納されており、したがって$\{Z_{d+1}(X_dx - Z_d) + X_{d+1}(X_d - xZ_d)\}(X_dx - Z_d)^2$が計算される。その結

果がレジスタ$T_1$に格納される。ステップ９１９において$T_1 \times T_3$が計算される。ここでレジスタ$T_1$には$\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$がレジスタ$T_3$には$Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)$が格納されており、したがって$\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$が計算される。その結果がレジスタ$Y_d$に格納される。したがってレジスタ$Y_d$には$\{Z_{d+1}(X_d x - Z_d) + X_{d+1}(X_d - xZ_d)\}\{Z_{d+1}(X_d x - Z_d) - X_{d+1}(X_d - xZ_d)\}(X_d x - Z_d)^2$が格納されている。レジスタ$X_d$にはステップ９１４において$ByZ_{d+1}X_{d+1}Z_{d+1}(X_d - xZ_d)^2 X_d$が格納され、その後更新が行われないので、その値が保持されている。レジスタ$Z_d$にはステップ９１５において$By\ Z_{d+1}X_{d+1}Z_{d+1}(X_d - xZ_d)^2 Z_d$が格納され、その後更新が行われないので、その値が保持されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からスカラー倍点の射影座標$(X_d, Y_d, Z_d)$における値が全て復元される理由は以下の通りである。点$(d+1)P$は点$dP$に点$P$を加算した点であり、点$(d-1)P$は点$dP$から点$P$を減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の数６、数７を得る。両辺を各々減算することにより、数８を得る。したがって、数９となる。ここで$x_d = X_d/Z_d$、$x_{d+1} = X_{d+1}/Z_{d+1}$、$x_{d-1} = X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、数１０を得る。

モンゴメリ型楕円曲線の射影座標での加算公式は数１１、数１２である。ここで$X_m$及び$Z_m$はモンゴメリ型楕円曲線上の点Pのm倍点mPの射影座標におけるX座標及びZ座標、$X_n$及び$Z_n$はモンゴメリ型楕円曲線上の点Pのｎ倍点nPの射影座標におけるX座標及びZ座標、$X_{m-n}$及び$Z_{m-n}$はモンゴメリ型楕円曲線上の点Pの(m-n)倍点(m-n)Pの射影座標におけるX座標及びZ座標、$X_{m+n}$及び$Z_{m+n}$はモンゴメリ型楕円曲線上の点Pの(m+n)倍点(m+n)Pの射影座標におけるX座標及びZ座標であり、$m$，$n$は$m > n$をみたす正整数である。この式は$X_m/Z_m = x_m$、$X_n/Z_n = x_n$、$X_{m-n}/Z_{m-n} = x_{m-n}$が不変のとき、$X_{m+n}/Z_{m+n} = x_{m+n}$も不変となるので、射影座標での公式としてうまく働いている。他方、数１４、数１５とおくと、この式で$X_m/Z_m = x_m$、$X_n/Z_n = x_n$、$X_{m+n}/Z_{m+n} = x_{m+n}$が

不変のとき、$X'_{m-n}/Z'_{m-n}$も不変となる。また、$X'_{m-n}/Z'_{m-n}=X_{m-n}/Z_{m-n}=x_{m-n}$をみたすので、$x_{m-n}$の射影座標として$X'_{m-n}, Z'_{m-n}$をとってよい。m=d、n=1として上記公式を用いて$y_d$の式より$X_{d-1}$及び$Z_{d-1}$を消去し、$X_1=x, Z_1=1$とおくことにより、数１５を得る。$x_d=X_d/Z_d$であるが、$y_d$の分母と通分することにより、数１６となる。

その結果として、

$$Y_d=\{Z_{d+1}(X_d x-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_d x-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_d x-Z_d)^2$$

…数１７

とし、$X_d$及び$Z_d$をそれぞれ

$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d$ …数１８

$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$ …数１９

により更新すればよい。ここで、$X_d$, $Y_d$, $Z_d$は図９の処理により与えられている。したがって、射影座標$(X_d, Y_d, Z_d)$の値が全て復元されていることになる。

上記手順はステップ９０１、ステップ９０３、ステップ９０５、ステップ９０６、ステップ９０９、ステップ９１０、ステップ９１１、ステップ９１２、ステップ９１３、ステップ９１４、ステップ９１５、ステップ９１８及びステップ９１９において有限体上の乗算の計算量を必要とする。また、ステップ９０７及びステップ９０８において有限体上の２乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をSとすると、上記手順は１３M＋２Sの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。S＝０．８Mと仮定すると座標復元の計算量は１４．６Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d$、$Y_d$、$Z_d$の値が計算できれば$X_d$、$Y_d$、$Z_d$の値が復元できる。また、$x_d$、$y_d$が上記計算式に

より与えられる値を取るように$X_d$、$Y_d$、$Z_d$の値を選択し、その値が計算できれば$X_d$、$Y_d$、$Z_d$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBの値を小さくとることにより、ステップ９１３における乗算の計算量を削減することができる。

次に、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムについて説明する。

第２実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第１実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記アルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１３Ｍ＋２Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ—４．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋１０）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１４８２Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第３の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点($x_d$, $y_d$)を計算し出力するものである。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力す

ると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたモンゴメリ型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点(d−1)P＝$(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点P=(x, y)と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$、x及びyよりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図１２により、座標x、y、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$が与えられた場合に$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標うち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)$P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点(d-1)P＝$(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d-1)Pのアフィン座標を$(x_{d-1}, y_{d-1})$で、射影座標を$(X_{d-1}, Y_{d-1}, Z_{d-1})$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ１２０１において$X_{d-1} \times Z_{d+1}$が計算され、レジスタＴ$_1$に格納される。ステップ１２０２において$Z_{d-1} \times X_{d+1}$が計算され、レジスタＴ$_2$に格納される。ステップ１２０３においてＴ$_1$－Ｔ$_2$が計算される。ここでレジスタＴ$_1$には$X_{d-1}Z_{d+1}$がレジスタＴ$_2$には$Z_{d-1}X_{d+1}$がそれぞれ格納されており、したがって$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ１２０４において$Z_d \times x$が計算され、レジスタＴ$_2$に格納される。ステップ１２０５において$X_d-$Ｔ$_2$が計算さる。ここでレジスタＴ$_2$には$Z_d x$が格納されており、したがって$X_d-xZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２０６においてＴ$_2$の２乗が計算される。ここでレジスタＴ$_2$には$X_d-xZ_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２０７においてＴ$_1$×Ｔ$_2$が計算される。ここでレジスタＴ$_1$には$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$がレジスタＴ$_2$には$(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ１２０８において４Ｂ×ｙが計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２０９においてＴ$_2 \times Z_{d+1}$が計算される。ここでレジスタＴ$_2$には$4By$が格納されており、したがって$4ByZ_{d+1}$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２１０においてＴ$_2 \times Z_{d-1}$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}$が格納されており、したがって$4ByZ_{d-1}Z_{d+1}$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２１１においてＴ$_2 \times Z_d$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}Z_{d-1}$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２１２においてＴ$_2 \times X_d$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d-1}Z_{d+1}Z_d$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dX_d$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ１２１３においてＴ$_2 \times Z_d$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１２１４においてレジスタＴ$_2$の逆元が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}Z_{d-1}Z_dZ_d$が

格納されており、したがって$1/4ByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１２１５において$T_2 \times T_3$が計算される。ここでレジスタ$T_2$には$1/4ByZ_{d+1}Z_{d-1}Z_dZ_d$がレジスタ$T_3$には$4ByZ_{d+1}Z_{d-1}Z_dX_d$ がそれぞれ格納されており、したがって$(4ByZ_{d+1}Z_{d-1}Z_dX_d)/(4ByZ_{d+1}Z_{d-1}Z_dZ_d)$が計算される。その結果がレジスタ$x_d$に格納される。ステップ１２１６において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$がレジスタ$T_2$には$1/4ByZ_{d+1}Z_{d-1}Z_dZ_d$がそれぞれ格納されており、したがって$(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2/4ByZ_{d-1}Z_{d+1}Z_d{}^2$が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には$(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2/4ByZ_{d-1}Z_{d+1}Z_d{}^2$が格納されている。レジスタ$x_d$にはステップ１２１５において$(4ByZ_{d+1}Z_{d-1}Z_dX_d)/(4ByZ_{d+1}Z_{d-1}Z_dZ_d)$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からモンゴメリ型楕円曲線におけるスカラー倍点のアフィン座標$(x_d, y_d)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点であり、点$(d-1)$Pは点dPから点Pを減算した点である。

モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６、数７を得る。両辺を各々減算することにより、数８を得る。したがって、数９となる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、数１０を得る。

$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、

$$x_d = \frac{4ByZ_{d+1}Z_{d-1}Z_dX_d}{4ByZ_{d+1}Z_{d-1}Z_dZ_d} \quad \cdots 数２０$$

となる。この$x_d$，$y_d$は図１２で示した処理により与えられ、したがってアフィン座標$(x_d, y_d)$の値が全て復元されていることになる。

上記手順はステップ１２０１、ステップ１２０２、ステップ１２０４、ステッ

プ１２０７、ステップ１２０８、ステップ１２０９、ステップ１２１０、ステップ１２１１、ステップ１２１２、ステップ１２１３、ステップ１２１５及びステップ１２１６において有限体上の乗算の計算量を必要とする。また、ステップ１２０６において有限体上の２乗算の計算量を必要とする。また、ステップ１２１４において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１２M＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M、Ｉ＝４０Mと仮定すると座標復元の計算量は５２．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$，$y_d$の値が計算できれば$x_d$，$y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBの値を小さくとることにより、ステップ１２０８における乗算の計算量を削減することができる。

次に図５により、スカラー値d及びモンゴメリ型楕円曲線上の点Pから$X_d$, $Z_d$, $X_{d+1}$, $Z_{d+1}$, $X_{d-1}$, $Z_{d-1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点(d-1)P＝$(X_{d-1}, Y_{d-1}, Z_{d-1})$のうち$X_{d-1}$及び$Z_{d-1}$を出力する。ステップ５０１として、変数Ｉに初期値１を代入する。ステップ５０２として、点Pの２

倍点２Pを計算する。ここで点Pは射影座標において(ｘ，ｙ，1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ５０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ５０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ５０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればm=dとなり、ステップ５１４へ行く。一致しなければステップ５０５へ行く。ステップ５０５として、変数Ｉを１増加させる。ステップ５０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ５０７へ行く。そのビットの値が１であればステップ５１０へ行く。ステップ５０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ５０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ５０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ５０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ５０９として、ステップ５０８で求めた点2mPとステップ５０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ５０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ５１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ５１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ５１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ５１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ５１２として、ステップ５１０で求めた点(2m+１)Pとステップ５１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組

(mP, (m+1)P)の代わりに格納する。その後ステップ５０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ５１４として、射影座標で表された点の組(mP, (m+1)P)から、点(m-1)Pの射影座標におけるX座標$X_{m-1}$及びZ座標$Z_{m-1}$を求め、それぞれ$X_{d-1}$及び$Z_{d-1}$とする。その後ステップ５１３へ行く。ステップ５１３として、射影座標で表された点mP＝($X_m$, $Y_m$, $Z_m$)より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$として、射影座標で表された点(m+1)P＝($X_{m+1}$, $Y_{m+1}$, $Z_{m+1}$)より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$として、$X_{d-1}$及び$Z_{d-1}$と共に出力する。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。また上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ５１４において(m-1)Pを求める際に、数１０、数１１の公式により求めてもよいし、ｍが奇数であれば、((m-1)/2)Pの値をステップ５１２の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の２倍算の公式より、(m-1)Pを求めてもよい。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1$＝１ととることにより３Ｍ＋２Ｓとなる。ここでMは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ５０７において加算の計算量、ステップ５０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ５１０において加算の計算量、ステップ５１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ５０４、ステップ５０５、ステップ５０６、ステップ５０７、ステップ５０８、ステップ５０９乃至はステップ５０４、ステップ５０５、ステップ５０６、ステップ５１０、ステップ５１１、ステップ５１２の繰り返しの回数は、（スカラー値ｄのビット長）－１回となるので、ステップ５０２での２倍算の計算量とステップ５１４での(m-1)Pの計算に必要な計算量を考慮に入れると、全体の計算

量は（６Ｍ＋４Ｓ）ｋ＋Ｍとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋１）Ｍとなる。例えばスカラー値ｄが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１４７３Ｍとなる。スカラー値dのビットあたりの計算量としてはおおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT' 98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６００Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$ ，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１２Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋１）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５３．８）Ｍと見積もることができる。例えばスカラー値ｄが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１５２６Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４

０Ｍであり、これと比べて必要となる計算量は削減されている。

第４の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算し出力する。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたモンゴメリ型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点$(_{d-1})P=(X_{d-1}, Y_{d-1}, Z_{d-1})$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$、x及びyよりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標$X_d, Y_d$及び$Z_d$の復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算結果として出力する。

次に図１３により、座標x、y $X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$が与えられた場合に$X_d$、$Y_d$、$Z_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d-1)P=(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した$(x, y)$を入力し、以下の手順で射影座標おいて完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を$(x, y)$で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$

で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d-1)Pのアフィン座標を$(x_{d-1}, y_{d-1})$で、射影座標を$(X_{d-1}, Y_{d-1}, Z_{d-1})$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ１３０１において$X_{d-1} \times Z_{d+1}$が計算され、レジスタ$T_1$に格納される。ステップ１３０２において$Z_{d-1} \times X_{d+1}$が計算され、レジスタ$T_2$に格納される。ステップ１３０３において$T_1 - T_2$が計算される。ここでレジスタ$T_1$には$X_{d-1}Z_{d+1}$がレジスタ$T_2$には$Z_{d-1}X_{d+1}$がそれぞれ格納されており、したがって$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１３０４において$Z_d \times x$が計算され、レジスタ$T_2$に格納される。ステップ１３０５において$X_d-T_2$が計算さる。ここでレジスタ$T_2$には$Z_d x$が格納されており、したがって$X_d-xZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１３０６において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$X_d-xZ_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１３０７において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$がレジスタ$T_2$には$(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が計算される。その結果がレジスタ$Y_d$に格納される。ステップ１３０８において$4B \times y$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１３０９において$T_2 \times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$4By$が格納されており、したがって$4ByZ_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１３１０において$T_2 \times Z_{d-1}$が計算される。ここでレジスタ$T_2$には$4ByZ_{d+1}$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１３１１において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$4ByZ_{d+1}Z_{d-1}$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１３１２において$T_2 \times X_d$が計算される。ここでレジスタ$T_2$には$4ByZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dX_d$が計算される。その結果がレジスタ$X_d$に格納され

る。ステップ１３１３において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$4ByZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果が$Z_d$に格納される。したがって$Z_d$には$4ByZ_{d+1}Z_{d-1}Z_dZ_d$が格納されている。レジスタ$Y_d$にはステップ１３０７において$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が格納され、その後更新が行われないので、その値が保持されている。

上記手順により与えられたｘ、ｙ、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からスカラー倍点の射影座標$(X_d, Y_d, Z_d)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。これより、先に述べた数７を得ることができる。座標復元部２０３はスカラー倍点の射影座標で表された完全な座標として$(X_d, Y_d, Z_d)$を出力する。

上記手順により与えられたx、y $X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からスカラー倍点の射影座標$(X_d, Y_d, Z_d)$における値が全て復元される理由は以下の通りである。点(ｄ＋１)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６、数７を得る。両辺を各々減算することにより、数８を得る。したがって、数９となる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、数７を得る。

$x_d=X_d/Z_d$であるが、$y_d$の分母と通分することにより、数２０となる。その結果として、

$$Y_d=(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2 \quad \cdots 数２１$$

とし、$X_d$及び$Z_d$をそれぞれ

$$4ByZ_{d+1}Z_{d-1}Z_dX_d \quad \cdots 数２２$$

$$4ByZ_{d+1}Z_{d-1}Z_dZ_d \quad \cdots 数２３$$

により更新すればよい。ここで示した$X_d$，$Y_d$，$Z_d$，は図１３で示した処理により与えられている。したがって、射影座標の値$(X_d, Y_d, Z_d)$が全て復元されていることになる。

上記手順はステップ１３０１、ステップ１３０２、ステップ１３０４、ステップ１３０７、ステップ１３０８、ステップ１３０９、ステップ１３１０、ステップ１３１１、ステップ１３１２及びステップ１３１３において有限体上の乗算の計算量を必要とする。また、ステップ１３０６において有限体上の２乗算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳとすると、上記手順は１０Ｍ＋Ｓの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００Ｍ弱と見積もられる。Ｓ＝０．８Ｍと仮定すると座標復元の計算量は１０．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d, Y_d, Z_d$の値が計算できれば$X_d, Y_d, Z_d$の値が復元できる。また、$x_d, y_d$が上記計算式により与えられる値を取るように$X_d, Y_d, Z_d$の値を選択し、その値が計算できれば$X_d$, $Y_d, Z_d$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメータであるBの値を小さくとることにより、ステップ１３０８における乗算の計算量を削減することができる。

次に、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムについて説明する。

第４実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第３実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量

は１０Ｍ＋Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋１）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋１１．８）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１４８４Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第５の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力する。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたモンゴメリ型楕円曲線上の点Pからモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d-1)P=(x_{d-1}, y_{d-1})$の座標のうち$x_{d-1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$x_d$、$x_{d+1}$、$x_{d-1}$、x及びyよりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図２６により、座標x、y、$x_d$、$x_{d+1}$、$x_{d-1}$が与えられた場合に、$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d-1)P＝$(x_{d-1}, y_{d-1})$の座標のうち$x_{d-1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。

ステップ２６０１において$x_d - x$が計算され、レジスタ$T_1$に格納される。ステップ２６０２において$T_1$の２乗すなわち$(x_d - x)^2$が計算され、レジスタ$T_1$に格納される。ステップ２６０３において$x_{d-1} - x_{d+1}$が計算され、レジスタ$T_2$に格納される。ステップ２６０４において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(x_d - x)^2$がレジスタ$T_2$には$x_{d-1} - x_{d+1}$がそれぞれ格納されており、したがって$(x_d - x)^2(x_{d-1} - x_{d+1})$が計算される。その結果がレジスタ$T_1$に格納される。ステップ２６０５において4B×yが計算され、レジスタ$T_2$に格納される。ステップ２６０６において$T_2$の逆元が計算される。ここでレジスタ$T_2$には4Byが格納されており、したがって1/4Byが計算される。その結果がレジスタ$T_2$に格納される。ステップ２６０７において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(x_d - x)^2(x_{d-1} - x_{d+1})$がレジスタ$T_2$には1/4Byがそれぞれ格納されており、したがって$(x_d - x)^2(x_{d-1} - x_{d+1})/4By$が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には$(x_d - x)^2(x_{d-1} - x_{d+1})/4By$が格納されている。レジスタ$x_d$は全く更新されないので入力された値が保持されている。

上記手順によりスカラー倍点のy座標$y_d$が復元される理由は以下の通りである。尚、点$(d+1)$Pは点dPに点Pを加算した点であり、点(d-1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６、数７を得る。

両辺を各々減算することにより、数８を得る。したがって、数９となる。

ここで、$x_d$，$y_d$は図２６の処理により与えられる。したがって、アフィン座標$(x_d, y_d)$の値は全て復元されたことになる。

上記手順はステップ２６０４、ステップ２６０５及びステップ２６０７において有限体上の乗算の計算量を必要とする。また、ステップ２６０２において有限体上の２乗算の計算量を必要とする。さらにステップ２６０６において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、２乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ、有限体上の逆元演算の計算量をＩとすると、上記手順は３Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M及びＩ＝４０Mと仮定すると座標復元の計算量は４３．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば$y_d$の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBの値を小さくとることにより、ステップ２６０５における乗算の計算量を削減することができる。

次に図６により、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$x_d$、$x_{d+1}$、$x_{d-1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(x_{d+1}, y_{d+1})$のうち$x_{d+1}$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d-1)P＝$(x_{d-1}, y_{d-1})$のうち$x_{d-1}$を出力する。ステップ６０１として、変数Ｉに初期値１を代入する。ステップ６０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(x, y, 1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ６０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ６０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表され

ている。ステップ６０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ６１４へ行く。一致しなければステップ６０５へ行く。ステップ６０５として、変数Ｉを１増加させる。ステップ６０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ６０７へ行く。そのビットの値が１であればステップ６１０へ行く。ステップ６０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ６０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ６０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ６０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ６０９として、ステップ６０８で求めた点2mPとステップ６０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ６０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ６１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ６１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ６１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ６１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ６１２として、ステップ６１０で求めた点(2m+１)Pとステップ６１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ６０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ６１４として、射影座標で表された点の組(mP, (m+1)P)から、点(m-1)Pの射影座標におけるX座標$X_{m-1}$及びZ座標$Z_{m-1}$を求め、それぞれ$X_{d-1}$及び$Z_{d-1}$とする。その後ステップ６１５へ行く。

ステップ６１５として、射影座標で表された点mP＝$(X_m, Y_m, Z_m)$より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$とし、射影座標で表された点(m+1)P＝$(X_{m+1}, Y_{m+1}, Z_{m+1})$より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$とする。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。$X_{d-1}$，$Z_{d-1}$，$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$より、

$$x_{d-1} = X_{d-1}Z_dZ_{d+1}/Z_{d-1}Z_dZ_{d+1} \quad \cdots 数２４$$

$$x_d = Z_{d-1}X_dZ_{d+1}/Z_{d-1}Z_dZ_{d+1} \quad \cdots 数２５$$

$$x_{d+1} = Z_{d-1}Z_dX_{d+1}/Z_{d-1}Z_dZ_{d+1} \quad \cdots 数２６$$

として$x_{d-1}$，$x_d$，$x_{d+1}$を求める。その後ステップ６１３へ行く。ステップ６１３として、$x_{d-1}$，$x_d$，$x_{d+1}$を出力する。上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ６１４において(m-1)Pを求める際に、数１３、数１４の公式により求めてもよいし、ｍが奇数であれば、((m-1)/2)Pの値をステップ６１２の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の２倍算の公式より、(m-1)Pを求めてもよい。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1$＝1ととることにより３Ｍ＋２Ｓとなる。ここでMは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ６０７において加算の計算量、ステップ６０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ６１０において加算の計算量、ステップ６１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ６０４、ステップ６０５、ステップ６０６、ステップ６０７、ステップ６０８、ステップ６０９乃至はステップ６０４、ステップ６０５、ステップ６０６、ステップ６１０、ステップ６１１、ステップ６１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ６０２での２倍算の計算量及

びステップ６１４での(m-1)Pの計算に必要な計算量及びアフィン座標への変換の計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋１１Ｍ＋Ｉとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度、計算量ＩはＩ＝４０Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋５１）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１５２３Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６４０Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$x_d$、$x_{d+1}$、$x_{d-1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は3Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋５１）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍ及びＩ＝４０Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋９４．８）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１５６７Ｍとなる。楕円

曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第６の実施例は、楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部１０３の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部１０３の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力するものである。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(_{d+1})P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d-1)P=(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$、ｘ及びｙよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図１４により、座標x、y、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$が与えられた場合に$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、ワイエルシュトラス型楕円曲線において射影座標で表

されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標うち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d+1)$P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(d-1)P＝$(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてワイエルシュトラス型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点(d-1)Pのアフィン座標を$(x_{d-1}, y_{d-1})$で、射影座標を$(X_{d-1}, Y_{d-1}, Z_{d-1})$でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ１４０１において$X_{d-1} \times Z_{d+1}$が計算され、レジスタ$T_1$に格納される。ステップ１４０２において$Z_{d-1} \times X_{d+1}$が計算され、レジスタ$T_2$に格納される。ステップ１４０３において$T_1 - T_2$が計算される。ここでレジスタ$T_1$には$X_{d-1}Z_{d+1}$がレジスタ$T_2$には$Z_{d-1}X_{d+1}$がそれぞれ格納されており、したがって$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１４０４において$Z_d \times x$が計算され、レジスタ$T_2$に格納される。ステップ１４０５において$X_d - T_2$が計算さる。ここでレジスタ$T_2$には$Z_d x$が格納されており、したがって$X_d - xZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４０６において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$X_d - xZ_d$が格納されており、したがって$(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４０７において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$がレジスタ$T_2$には$(X_d - xZ_d)^2$がそれぞれ格納されており、したがって$(X_d - xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１４０８において$4 \times y$が計算される。その結果がレ

ジスタ$T_2$に格納される。ステップ１４０９において$T_2 \times Z_{d+1}$が計算される。ここでレジスタ$T_2$には4yが格納されており、したがって$4yZ_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４１０において$T_2 \times Z_{d-1}$が計算される。ここでレジスタ$T_2$には$4yZ_{d+1}$が格納されており、したがって$4yZ_{d+1}Z_{d-1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４１１において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$4yZ_{d+1}Z_{d-1}$が格納されており、したがって$4yZ_{d+1}Z_{d-1}Z_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４１２において$T_2 \times X_d$が計算される。ここでレジスタ$T_2$には$4yZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4yZ_{d+1}Z_{d-1}Z_dX_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ１４１３において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$4yZ_{d-1}Z_{d+1}Z_d$が格納されており、したがって$4yZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４１４においてレジスタ$T_2$の逆元が計算される。ここでレジスタ$T_2$には$4yZ_{d+1}Z_{d-1}Z_dZ_d$が格納されており、したがって$1/4yZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４１５において$T_2 \times T_3$が計算される。ここでレジスタ$T_2$には$1/4yZ_{d+1}Z_{d-1}Z_dZ_d$がレジスタ$T_3$には$4yZ_{d-1}Z_{d+1}Z_dX_d$がそれぞれ格納されており、したがって$(4yZ_{d+1}Z_{d-1}Z_dX_d)/(4yZ_{d+1}Z_{d-1}Z_dZ_d)$が計算される。その結果が$x_d$に格納される。ステップ１４１６において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(X_d - xZ_d)^2(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})$がレジスタ$T_2$には$1/4yZ_{d+1}Z_{d-1}Z_dZ_d$がそれぞれ格納されており、したがって$(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2/4yZ_{d+1}Z_{d-1}Z_d^2$が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には$(X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_dx)^2/4yZ_{d-1}Z_{d+1}Z_d^2$が格納されている。レジスタ$x_d$にはステップ１４１５において$(4yZ_{d-1}Z_{d+1}Z_dX_d)/(4yZ_{d-1}Z_{d+1}Z_dZ_d)$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられたx、y、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標

($x_d$, $y_d$)における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、次の式を得る。

$$(x+x_d+x_{d+1})(x_d-x)^2=(y_d-y)^2 \quad \cdots 数２７$$

$$(x+x_d+x_{d-1})(x_d-x)^2=(y_d+y)^2 \quad \cdots 数２８$$

両辺を各々減算することにより、

$$(x_{d-1}-x_{d+1})(x_d-x)^2=4y_d y \quad \cdots 数２９$$

を得る。したがって、

$$y_d=(x_{d-1}-x_{d+1})(x_d-x)^2/4y \quad \cdots 数３０$$

となる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d=1}=X_{d=1}/Z_{d=1}$であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d=(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_d x)^2/4yZ_{d-1}Z_{d+1}Z_d^2 \quad \cdots 数３１$$

$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、

$$x_d=\frac{4yZ_{d+1}Z_{d-1}Z_dX_d}{4yZ_{d+1}Z_{d-1}Z_dZ_d} \quad \cdots 数３２$$

となる。ここで、$x_d$, $y_d$は図１４で示した処理により与えられる。したがって、アフィン座標($x_d$, $y_d$)の値が全て復元されていることになる。

上記手順はステップ１４０１、ステップ１４０２、ステップ１４０４、ステップ１４０７、ステップ１４０９、ステップ１４１０、ステップ１４１１、ステップ１４１２、ステップ１４１３、ステップ１４１５及びステップ１４１６において有限体上の乗算の計算量を必要とする。ただし、ステップ１４０８の乗算は、被乗数の値が４と小さいので、その計算量は通常の乗算の計算量と比べて小さい為無視してよい。また、ステップ１４０６において有限体上の２乗算の計算量を必要とする。また、ステップ１４１４において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の

乗算の計算量をM、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１１M＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M、Ｉ＝４０Mと仮定すると座標復元の計算量は５１．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$，$y_d$の値が計算できれば$x_d$，$y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。

次に図７により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d, Z_d, X_{d+1}, Z_{d+1}, X_{d-1}, Z_{d-1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(ｄ－１)P＝$(X_{d-1}, Y_{d-1}, Z_{d-1})$のうち$X_{d-1}$及び$Z_{d-1}$を出力する。ステップ７１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ７０１として、変数Ｉに初期値１を代入する。ステップ７０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(ｘ，ｙ，1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ７０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ７０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ７０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ７１４へ行く。一致しなければステップ７

０５へ行く。ステップ７０５として、変数Ｉを１増加させる。ステップ７０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ７０７へ行く。そのビットの値が１であればステップ７１０へ行く。ステップ７０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ７０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ７０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ７０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ７０９として、ステップ７０８で求めた点2mPとステップ７０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ７０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ７１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ７１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ７１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ７１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ７１２として、ステップ７１０で求めた点(2m+１)Pとステップ７１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ７０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ７１４として、射影座標で表された点の組 (mP, (m+1)P) から、点(m−1)Pの射影座標におけるX座標$X_{m-1}$及びZ座標$Z_{m-1}$を求める。その後ステップ７１５へ行く。ステップ７１５として、モンゴメリ型楕円曲線における点(m−1)Pを、ワイエルシュトラス型楕円曲線上で射影座標により表された点に変換する。その点のX座標及びZ座標をそれぞれあらためて

$X_{m-1}$及び$Z_{m-1}$とおく。また、モンゴメリ型楕円曲線において射影座標で表された点の組(mP, (m+1)P)に対して、点mP及び点(m+1)Pをワイエルシュトラス型楕円曲線上で射影座標で表された点に変換し、それぞれmP＝（$X_m$, $Y_m$, $Z_m$）及び(m+1)P＝（$X_{m+1}$, $Y_{m+1}$, $Z_{m+1}$）とあらためて置き直す。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。ステップ７１３として、ワイエルシュトラス型楕円曲線上で射影座標で表された点(m-1)PのX座標$X_{m-1}$及びZ座標$Z_{m-1}$をそれぞれ$X_{d-1}$及び$Z_{d-1}$として、ワイエルシュトラス型楕円曲線上で射影座標で表された点mP＝（$X_m$, $Y_m$, $Z_m$）より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$として、ワイエルシュトラス型楕円曲線上で射影座標で表された点(m+1)P＝（$X_{m+1}$, $Y_{m+1}$, $Z_{m+1}$）より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$として、出力する。また上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ７１４において(m-1)Pを求める際に、数１３、数１４の公式により求めてもよいし、ｍが奇数であれば、((m-1)/2)Pの値をステップ７１２の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の２倍算の公式より、(m-1)Pを求めてもよい。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1$=1ととることにより３Ｍ＋２Ｓとなる。ここでＭは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ７０７において加算の計算量、ステップ７０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ７１０において加算の計算量、ステップ７１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ７０４、ステップ７０５、ステップ７０６、ステップ７０７、ステップ７０８、ステップ７０９乃至はステップ７０４、ステップ７０５、ステップ７０６、ステップ７１０、ステップ７１１、ステップ７１２の繰り返しの回数は、（スカ

ラー値dのビット長）－１回となるので、ステップ７０２での２倍算の計算量とステップ７１６でのモンゴメリ型楕円曲線上の点への変換に必要な計算量及びステップ７１５でのワイエルシュトラス型楕円曲線上の点への変換に必要な計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋４Ｍとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋４）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１４７６Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６００Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１１Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋４）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５５．８）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１５２８Ｍとなる。楕円曲

線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第７の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部１０３の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部１０３の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d-1)P=(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$、x及びyよりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標$X_d, Y_d$及び$Z_d$の復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算結果として出力する。

次に図１５により、座標x、y $X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$が与えられた場合に$X_d$、$Y_d$、$Z_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、ワイエルシュトラス型楕円曲線において射影座標で表

されたスカラー倍点dP＝($X_d$, $Y_d$, $Z_d$)の座標のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(d-1)P＝($X_{d-1}$, $Y_{d-1}$, $Z_{d-1}$)の座標のうち$X_{d-1}$及び$Z_{d-1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順で射影座標おいて完全な座標が与えられたスカラー倍点($X_d$, $Y_d$, $Z_d$)を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を($X_1$, $Y_1$, $Z_1$)でそれぞれ表す。入力されたスカラー値をdとしてワイエルシュトラス型楕円曲線におけるスカラー倍点dPのアフィン座標を($x_d$, $y_d$)で、射影座標を($X_d$, $Y_d$, $Z_d$)でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点(d-1)Pのアフィン座標を($x_{d-1}$, $y_{d-1}$)で、射影座標を($X_{d-1}$, $Y_{d-1}$, $Z_{d-1}$)でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点(d+1)Pのアフィン座標を($x_{d+1}$, $y_{d+1}$)で、射影座標を($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)でそれぞれ表す。

ステップ１５０１において$X_{d-1}\times Z_{d+1}$が計算され、$T_1$に格納される。ステップ１５０２において$Z_{d-1}\times X_{d+1}$が計算され、$T_2$に格納される。ステップ１５０３において$T_1-T_2$が計算される。ここで$T_1$には$X_{d-1}Z_{d+1}$が$T_2$には$Z_{d-1}X_{d+1}$がそれぞれ格納されており、したがって$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が計算される。その結果が$T_1$に格納される。ステップ１５０４において$Z_d\times x$が計算され、$T_2$に格納される。ステップ１５０５において$X_d-T_2$が計算さる。ここで$T_2$には$Z_d x$が格納されており、したがって$X_d-xZ_d$が計算される。その結果が$T_2$に格納される。ステップ１５０６において$T_2$の２乗が計算される。ここで$T_2$には$X_d-xZ_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果が$T_2$に格納される。ステップ１５０７において$T_1\times T_2$が計算される。ここで$T_1$には$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が$T_2$には$(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$(X_d-xZ_d)2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が計算される。その結果がレジスタ$Y_d$に格納される。ステップ１５０８において$4\times y$が計算される。その結果が$T_2$に格納される。ステップ１５０９において$T_2\times Z_{d+1}$が計算される。ここで$T_2$には4yが格納されており、したが

って$4yZ_{d+1}$が計算される。その結果が$T_2$に格納される。ステップ１５１０において$T_2 \times Z_{d-1}$が計算される。ここで$T_2$には$4yZ_{d+1}$が格納されており、したがって$4yZ_{d+1}Z_{d-1}$が計算される。その結果が$T_2$に格納される。ステップ１５１１において$T_2 \times Z_d$が計算される。ここで$T_2$には$4yZ_{d+1}Z_{d-1}$が格納されており、したがって$4yZ_{d+1}Z_{d-1}Z_d$が計算される。その結果が$T_2$に格納される。ステップ１５１２において$T_2 \times X_d$が計算される。ここで$T_2$には$4yZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4yZ_{d+1}Z_{d-1}Z_dX_d$が計算される。その結果がレジスタXdに格納される。ステップ１５１３において$T_2 \times Z_d$が計算される。ここで$T_2$には$4yZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4yZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタ$Z_d$に格納される。したがってレジスタ$Z_d$には$4y\ Z_{d+1}Z_{d-1}Z_dZ_d$が格納されている。レジスタ$Y_d$にはステップ１５０７において$(X_d-xZ_d)2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が格納され、その後更新が行われないので、その値が保持されている。レジスタ$X_d$にはステップ１５１２において$4yZ_{d+1}Z_{d-1}Z_dX_d$が格納され、その後更新が行われないので、その値が保持されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標$(X_d, Y_d, Z_d)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数２７、数２８を得る。両辺を各々減算することにより、数２９を得る。したがって、数３０となる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、数３１を得る。$x_d=X_d/Z_d$であるが、$y_d$の分母と通分することにより、数３２となる。

その結果として

$$Y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 \quad \cdots 数３３$$

とし、$X_d$及び$Z_d$をそれぞれ

$$4yZ_{d+1}Z_{d-1}Z_dX_d \quad \cdots 数３４$$

$4yZ_{d+1}Z_{d-1}Z_dZ_d$ …数３５

により更新すればよい。

ここで、$X_d$，$Y_d$，$Z_d$は図１５で示した処理により与えられる。したがって、射影座標($X_d$,$Y_d$,$Z_d$)の値は全て復元されたことになる。

上記手順はステップ１５０１、ステップ１５０５、ステップ１５０４、ステップ１５０７、ステップ１５０９、ステップ１５１０、ステップ１５１１、ステップ１５１２及びステップ１５１３において有限体上の乗算の計算量を必要とする。ただし、ステップ１５０８の乗算は、被乗数の値が４と小さいので、その計算量は通常の乗算の計算量と比べて小さい為無視してよい。また、ステップ１５０６において有限体上の２乗算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳとすると、上記手順は９M＋Ｓの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８Mと仮定すると座標復元の計算量は９．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d$,$Y_d$,$Z_d$の値が計算できれば$X_d$,$Y_d$,$Z_d$の値が復元できる。また、$x_d$,$y_d$が上記計算式により与えられる値を取るように$X_d$,$Y_d$,$Z_d$の値を選択し、その値が計算できれば$X_d$,$Y_d$,$Z_d$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムについて説明する。

第７実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第６実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は９Ｍ＋Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋４）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋１３．８）Ｍと見積もることができる。例えばスカラー値ｄが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１４８６Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第８の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部１０３の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部１０３の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝

$(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d-1)P＝$(x_{d-1}, y_{d-1})$の座標のうち$x_{d-1}$を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点P＝(x, y)と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$x_d$、$x_{d+1}$、$x_{d-1}$、x及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図１６により、座標x、y、$x_d$、$x_{d+1}$、$x_{d-1}$が与えられた場合に、$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、ワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝$(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d-1)P＝$(x_{d-1}, y_{d-1})$の座標のうち$x_{d-1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。

ステップ１６０１において$x_d$－xが計算され、$T_1$に格納される。ステップ１６０２において$T_1$の２乗すなわち$(x_d-x)^2$が計算され、$T_1$に格納される。ステップ１６０３において$x_{d-1}-x_{d+1}$が計算され、$T_2$に格納される。ステップ１６０４において$T_1 \times T_2$が計算される。ここで$T_1$には$(x_d-x_2$が$T_2$には$x_{d-1}-x_{d+1}$がそれぞれ格納されており、したがって$(x_d-x)^2(x_{d-1}-x_{d+1})$が計算される。その結果が$T_1$に格納される。ステップ１６０５において4×yが計算され、$T_2$に格納される。ステップ１６０６において$T_2$の逆元が計算される。ここで$T_2$には4yが格納されており、したがって1/4yが計算される。その結果が$T_2$に格納される。ステップ１６０７において$T_1 \times T_2$が計算される。ここで$T_1$には$(x_d-x)^2(x_{d-1}-x_{d+1})$が$T_2$には1/4yがそれぞれ格納されており、したがって$(x_d-x)^2(x_{d-1}-x_{d+1})/4y$が計算される。その結果が

レジスタ$y_d$に格納される。したがってレジスタ$y_d$には$(x_d-x)^2(x_{d-1}-x_{d+1})/4y$が格納されている。レジスタ$x_d$は全く更新されないので入力された値が保持されている。

上記手順によりスカラー倍点のy座標$y_d$が復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数２７、数２８を得る。両辺を各々減算することにより、数２９を得る。したがって、数３０となる。ここで$x_d$, $y_d$は図１６の処理によって与えられる。したがって、アフィン座標$(x_d, y_d)$の値を全て復元していることになる。

上記手順はステップ１６０４、ステップ１６０７において有限体上の乗算の計算量を必要とする。ただし、ステップ１６０５の乗算は、被乗数の値が４と小さいので、その計算量は通常の乗算の計算量と比べて小さい為無視してよい。また、ステップ１６０２において有限体上の２乗算の計算量を必要とする。さらにステップ１６０６において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、２乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ、有限体上の逆元演算の計算量をＩとすると、上記手順は2M＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M及びＩ＝４０Mと仮定すると座標復元の計算量は４２．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば$y_d$の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。

次に図７により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$、$x_{d+1}$、$x_{d-1}$を出力するアルゴリズムについて説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりワイエルシュト

ラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝($x_d$, $y_d$)のうち$x_d$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝($x_{d+1}$, $y_{d+1}$)のうち$x_{d+1}$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d-1)P＝($x_{d-1}$, $y_{d-1}$)のうち$x_{d-1}$を出力する。ステップ７１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ７０１として、変数Ｉに初期値１を代入する。ステップ７０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(ｘ，ｙ,1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ７０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ７０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ７０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればm=dとなり、ステップ７１４へ行く。一致しなければステップ７０５へ行く。ステップ７０５として、変数Ｉを１増加させる。ステップ７０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ７０７へ行く。そのビットの値が１であればステップ７１０へ行く。ステップ７０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ７０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ７０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ７０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ７０９として、ステップ７０８で求めた点2mPとステップ７０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ７０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ７１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+

１)Pを計算する。その後ステップ７１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ７１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ７１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ７１２として、ステップ７１０で求めた点(2m+１)Pとステップ７１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ７０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ７１４として、射影座標で表された点の組(mP, (m+1)P)から、点(m−1)Pの射影座標におけるX座標Xm−1及びZ座標Zm−1を求める。その後ステップ７１５へ行く。ステップ７１５として、モンゴメリ型楕円曲線における点(m−1)Pを、ワイエルシュトラス型楕円曲線上でアフィン座標により表された点に変換する。その点のx座標をそれぞれあらためてxm−1とおく。また、モンゴメリ型楕円曲線において射影座標で表された点の組(mP, (m+1)P)に対して、点mP及び点(m+1)Pをワイエルシュトラス型楕円曲線上でアフィン座標で表された点に変換し、それぞれmP＝（xm, ym）及び(m+1)P＝（xm+1, ym+1）とあらためて置き直す。ここで、ym及びym+1は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。その後ステップ７１３へ行く。ステップ７１３として、ワイエルシュトラス型楕円曲線上でアフィン座標で表された点(m−1)Pのx座標xm−1を$x_{d-1}$として、ワイエルシュトラス型楕円曲線上で射影座標で表された点mP＝（$x_m, y_m$）より$x_m$を$x_d$として、ワイエルシュトラス型楕円曲線上でアフィン座標で表された点(m+1)P＝（$x_{m+1}$, $y_{m+1}$）より$x_{m+1}$を$x_{d+1}$として、出力する。また上記手順により、mとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ７１４において(m−1)Pを求める際に、数１３、数１４の公式により求めてもよいし、mが奇数であれば、((m−1)/2)Pの値をステップ７１２の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の２倍算の公式より、(m−1)Pを求めてもよい。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、Z1＝１ととることにより３M＋２Sとなる。ここでMは有限体上の乗算の計算量、Sは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３M＋２Sである。スカラー値のI番目のビットの値が０であれば、ステップ７０７において加算の計算量、ステップ７０８において２倍算の計算量が必要となる。すなわち６M＋４Sの計算量が必要となる。スカラー値のI番目のビットの値が１であれば、ステップ７１０において加算の計算量、ステップ７１１において２倍算の計算量が必要となる。すなわち６M＋４Sの計算量が必要である。いずれの場合においても６M＋４Sの計算量が必要である。ステップ７０４、ステップ７０５、ステップ７０６、ステップ７０７、ステップ７０８、ステップ７０９乃至はステップ７０４、ステップ７０５、ステップ７０６、ステップ７１０、ステップ７１１、ステップ７１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ７０２での２倍算の計算量とステップ７１６でのモンゴメリ型楕円曲線上への点への変換に必要な計算量及びステップ７１５でのワイエルシュトラス型楕円曲線上の点への必要な計算量を考慮に入れると、全体の計算量は（６M＋４S）k＋１５M＋Iとなる。ここでkはスカラー値dのビット長である。一般的には、計算量Sは、S＝０．８M程度、計算量Iは、I＝４０M程度と見積もられるので、全体の計算量はおおよそ（９．２k＋５５）Mとなる。例えばスカラー値dが１６０ビット（k＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１５２７Mとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Mとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Mと見積もられる。例えばスカラー値dが１６０ビット（k＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６４０Mとなる。したがって、上記手順のアルゴリズムの方が計算量が少

なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$, $x_{d+1}$, $x_{d=1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は2M＋S＋Iであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋５５）Mとに比べてはるかに小さい。じたがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。I＝４０M、S＝０．８Mと仮定すると、この計算量はおおよそ（９．２ｋ＋９７．８）Mと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１５７０Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Mであり、これと比べて必要となる計算量は削減されている。

第９の実施例は、入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点（$x_d$, $y_d$）を計算し出力するものである。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値ｄと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝($X_d$, $Y_d$, $Z_d$)の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$）の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算する。また、入力されたワ

イエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たにP＝(x, y)とおく。高速スカラー倍計算部２０２は、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、ｘ及びｙを座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、ｘ及びｙよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝($x_d$, $y_d$)の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点($x_d$, $y_d$)を計算結果として出力する。

次に図１７により、座標x, y, $X_d$, $Z_d$, $X_{d+1}$, $Z_{d+1}$が与えられた場合に$x_d$, $y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝($X_d$, $Y_d$, $Z_d$)の座標うち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点($x_d$, $y_d$)を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を(X１, Y１, Z１)でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を($x_d^{Mon}$, $y_d^{Mon}$)で、射影座標を($X_d$, $Y_d$, $Z_d$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d−1)Pのアフィン座標を($x_{d-1}$, $y_{d-1}$)で、射影座標を($X_{d-1}$, $Y_{d-1}$, $Z_{d-1}$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を($x_{d+1}$, $y_{d+1}$)で、射影座標を($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)でそれぞれ表す。

ステップ１７０１において$X_d$×xが計算され、レジスタ$T_1$に格納される。ステップ１７０２において$T_1$-$Z_d$が計算される。ここでレジスタ$T_1$には$X_d$xが格納されており、したがって$X_d$x-$Z_d$ が計算される。その結果がレジスタ$T_1$に格納される。ステップ１７０３において$Z_d$×xが計算され、レジスタ$T_2$に格納される。ステップ１７０４において$X_d$−$T_2$が計算される。ここでレジスタ$T_2$には$Z_d$xが格納されており、したがって$X_d$-x$Z_d$が計算される。その結果がレジ

スタＴ$_2$に格納される。ステップ１７０５において$X_{d+1}$×Ｔ$_2$が計算される。ここでレジスタＴ$_2$には$X_d$-x$Z_d$が格納されており、したがって$X_{d+1}$($X_d$-x$Z_d$)が計算される。その結果がレジスタＴ$_3$に格納される。ステップ１７０６においてＴ$_2$の２乗が計算される。ここでレジスタＴ$_2$には($X_d$-x$Z_d$)が格納されており、したがって($X_d$-x$Z_d$)$^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７０７においてＴ$_2$×$X_{d+1}$が計算される。ここでレジスタＴ$_2$には($X_d$-x$Z_d$)$^2$が格納されており、したがって$X_{d+1}$($X_d$-x$Z_d$)$^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７０８においてＴ$_2$×$Z_{d+1}$が計算される。ここでレジスタＴ$_2$には$X_{d+1}$($X_d$-x$Z_d$)$^2$が格納されており、したがって$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７０９においてＴ$_2$×yが計算される。ここでレジスタＴ$_2$には$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2$が格納されており、したがってy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７１０においてＴ$_2$×Bが計算される。ここでレジスタＴ$_2$にはy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2$が格納されており、したがってBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７１１においてＴ$_2$×$Z_d$が計算される。ここでレジスタＴ$_2$にはBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2$が格納されており、したがってBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７１２においてＴ$_2$×$X_d$が計算される。ここでレジスタＴ$_2$にはBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$が格納されており、したがってBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_dX_d$が計算される。その結果がレジスタＴ$_4$に格納される。ステップ１７１３においてＴ$_2$×$Z_d$が計算される。ここでレジスタＴ$_2$にはBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$が格納されており、したがってBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７１４においてレジスタＴ$_2$×sが計算される。ここでレジスタＴ$_2$にはBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$2が格納されており、したがってsBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$2が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７１５においてＴ$_2$の逆元が計算される。ここで、Ｔ$_2$にはsBy$Z_{d+1}X_{d+1}$($X_d$-x$Z_d$)$^2Z_d$2が格納されており、したがって1/ sBy$Z_{d+1}$

$X_{d+1}(X_d-xZ_d)^2Z_d2$が計算される。その結果がＴ$_2$に格納される。ステップ１７１６においてＴ$_2$×Ｔ$_4$が計算される。ここでレジスタＴ$_2$には$1/sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d2$がレジスタＴ$_4$には$ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d$がそれぞれ格納されており、したがって$(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d)/(sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2)$が計算される。その結果がレジスタＴ$_4$に格納される。ステップ１７１７においてＴ$_4+\alpha$が計算される。ここでレジスタＴ$_4$には$(ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_dX_d)/(sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2)$が格納されており、従って、数３６が計算される。

$$\frac{ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d}{sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d}+\alpha \quad \cdots 数３６$$

その結果が、レジスタ$x_d$に格納される。ステップ１７１８においてＴ$_1$×$Z_{d+1}$が計算される。ここでレジスタＴ$_1$には$X_dx-Z_d$が格納されており、したがって$Z_{d+1}(X_dx-Z_d)$が計算される。その結果がレジスタＴ$_4$に格納される。ステップ１７１９においてレジスタＴ$_1$の２乗が計算される。ここでレジスタＴ$_1$には$(X_dx-Z_d)$が格納されており、したがって$(X_dx-Z_d)^2$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ１７２０においてＴ$_1$×Ｔ$_2$が計算される。ここでレジスタＴ$_1$には$(X_dx-Z_d)^2$がレジスタＴ$_2$には$1/sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$がそれぞれ格納されており、したがって$(X_dx-Z_d)^2/sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１７２１においてＴ$_3$+Ｔ$_4$が計算される。ここでレジスタＴ$_3$には$X_{d+1}(X_d-xZ_d)$ がレジスタＴ$_4$には$Z_{d+1}(X_dx-Z_d)$がそれぞれ格納されており、したがって$X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ１７２２においてＴ$_3$−Ｔ$_4$が計算される。ここでレジスタＴ$_3$には$X_{d+1}(X_d-xZ_d)$がレジスタＴ$_4$には$Z_{d+1}(X_dx-Z_d)$がそれぞれ格納されており、したがって$X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ１７２３においてＴ$_1$×Ｔ$_3$が計算される。ここでレジスタＴ$_1$には$X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)$がレジスタＴ$_3$には$X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)$がそれぞれ格納されており、したがって$\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-$

$Z_d$)}が計算される。その結果がレジスタ$T_1$に格納される。ステップ１７２４において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$\{X_{d+1}(X_d-xZ_d)+Z_{d+1}(X_dx-Z_d)\}\{X_{d+1}(X_d-xZ_d)-Z_{d+1}(X_dx-Z_d)\}$がレジスタ$T_2$には$(X_dx-Z_d)^2/sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2$がそれぞれ格納されており、したがって

$$\frac{\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2}{sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2}$$

…数３７

が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には数３７の値が格納されている。レジスタ$x_d$にはステップ１７１７において数３６の値が格納され、その後更新が行なわれないので、その値が保持されている。その結果として、ワイエルシュトラス型楕円曲線におけるアフィン座標($x_d$, $y_d$)の値が全て復元されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標($x_d$, $y_d$)における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d−1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の式を得る。

$$(A+x+x_d^{Mon}+x_{d+1})(x_d^{Mon}-x)^2 = B(y_d^{Mon}-y)^2 \quad \cdots 数３８$$

$$(A+x+x_d^{Mon}+x_{d-1})(x_d^{Mon}-x)^2 = B(y_d^{Mon}+y)^2 \quad \cdots 数３９$$

両辺を各々減算することにより、

$$(x_{d-1}-x_{d+1})(x_d^{Mon}-x)^2 = 4By_d^{Mon}y \quad \cdots 数４０$$

を得る。したがって、

$$y_d^{Mon} = (x_{d-1}-x_{d+1})(x_d^{Mon}-x)^2/4By \quad \cdots 数４１$$

となる。ここで$x_d^{Mon}=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d^{Mon} = (X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2/4ByZ_{d-1}Z_{d+1}Z_d^2 \quad \cdots 数４２$$

モンゴメリ型楕円曲線の射影座標での加算公式は既に示した数１１、数１２である。ここで$X_m$及び$Z_m$はモンゴメリ型楕円曲線上の点Pのｍ倍点mPの射影座標に

おけるX座標及びZ座標、$X_n$及び$Z_n$はモンゴメリ型楕円曲線上の点Pのn倍点nPの射影座標におけるX座標及びZ座標、$X_{m-n}$及び$Z_{m-n}$はモンゴメリ型楕円曲線上の点Pの(m-n)倍点(m-n)Pの射影座標におけるX座標及びZ座標、$X_{m+n}$及び$Z_{m+n}$はモンゴメリ型楕円曲線上の点Pの(m+n)倍点(m+n)Pの射影座標におけるX座標及びZ座標であり、m，nはm＞nをみたす正整数である。この式は$X_m/Z_m=x_m$、$X_n/Z_n=x_n$、$X_{m-n}/Z_{m-n}=x_{m-n}$が不変のとき、$X_{m+n}/Z_{m+n}=x_{m+n}$も不変となるので、射影座標での公式としてうまく働いている。他方、数１３、数１４とおくと、この式も$X_m/Z_m=x_m$、$X_n/Z_n=x_n$、$X_{m-n}/Z_{m-n}=x_{m-n}$が不変のとき、$X_{m+n}/Z_{m+n}=x_{m-n}$も不変となる。また、$X'_{m-n}/Z'_{m-n}=X_{m-n}/Z_{m-n}=x_{m-n}$をみたすので、$x_{m-n}$の射影座標として$X'_{m-n}, Z'_{m-n}$をとってよい。m=d、n=1として上記公式を用いて$y_d^{Mon}$の式より$X_{d-1}$及び$Z_{d-1}$を消去し、X1=x, Z1=1とおくことにより、次の式を得る。

$$y_d^{Mon}=\frac{\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2}{ByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2}$$

…数４３

$x_d^{Mon}=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d^{Mod}$の分母と通分することにより、

$$x_d^{Mon}=\frac{ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d}{ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d} \quad \text{…数４４}$$

となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをs, αとして、$y_d=s^{-1}y_d^{Mon}$及び$x_d=s^{-1}x_d^{Mon}+\alpha$の関係がある。結果として数４５、数４６を得る。

$$y_d=\frac{\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2}{sByZ_{d+1}X_{d+1}(X_d-xZ_d)^2Z_d^2}$$

…数４５

$$x_d = (ByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 X_d)/(sByZ_{d+1}X_{d+1}Z_d(X_d - xZ_d)^2 Z_d) + \alpha$$

…数４６

ここで、$x_d, y_d$は図１７より与えられる。したがって、ワイエルシュトラス型楕円曲線におけるアフィン座標($x_d, y_d$)の値が全て復元されていることになる。

上記手順はステップ１７０１、ステップ１７０３、ステップ１７０５、ステップ１７０７、ステップ１７０８、ステップ１７０９、ステップ１７１０、ステップ１７１１、ステップ１７１２、ステップ１７１３、ステップ１７１４、ステップ１７１６、ステップ１７１８、ステップ１７２０、ステップ１７２３及びステップ１７２４において有限体上の乗算の計算量を必要とする。また、ステップ１７０６及びステップ１７１９において有限体上の２乗算の計算量を必要とする。また、ステップ１７１５において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１６Ｍ＋２Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８Ｍ、Ｉ＝４０Ｍと仮定すると座標復元の計算量は５７．６Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$，$y_d$の値が計算できれば$x_d$，$y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタであるBの値やモンゴメリ型楕円曲線への変換パラメタであるｓを小さくとることにより、ステップ１７１０における乗算の計算量やステップ１７１４における乗算の計算量を削減することができる。

次に図８により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力する高速スカラー倍計算部の処理について説明

する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP=($X_d$, $Y_d$, $Z_d$)のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P=($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)のうち$X_{d+1}$及び$Z_{d+1}$を出力する。ステップ８１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ８０１として、変数Ｉに初期値１を代入する。ステップ８０２として、点Pの２倍点2Pを計算する。ここで点Pは射影座標において(x, y, 1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ８０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ８０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ８０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ８１３へ行く。一致しなければステップ８０５へ行く。ステップ８０５として、変数Ｉを１増加させる。ステップ８０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ８０７へ行く。そのビットの値が１であればステップ８１０へ行く。ステップ８０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ８０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ８０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算2(mP)を行ない、点2mPを計算する。その後ステップ８０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ８０９として、ステップ８０８で求めた点2mPとステップ８０７で求めた点(2m+1)Pを点の組(2mP, (2m+1)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ８０４へ戻る。ここで、点2mP、点(2m＋1)、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ８１０として、

射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)を計算する。その後ステップ８１１へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ８１１として、射影座標により表された点の組(mP, (m+1)P)から点(m+1)Pの２倍算2((m+1)P)を行ない、点(2m+2)Pを計算する。その後ステップ８１２へ行く。ここで、２倍算2((m+1)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ８１２として、ステップ８１０で求めた点(2m+1)Pとステップ８１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ８０４へ戻る。ここで、点(2m+1)P、点(2m+2)、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ８１３として、射影座標で表された点の組(mP, (m+1)P)から、射影座標で表された点$mP=(X_m, Y_m, Z_m)$より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$として、射影座標で表された点$(m+1)P=(X_{m+1}, Y_{m+1}, Z_{m+1})$より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$として、出力する。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。また上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、Z1=1ととることにより３Ｍ＋２Ｓとなる。ここでMは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ８０７において加算の計算量、ステップ８０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ８１０において加算の計算量、ステップ８１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ８０４、ステップ８０５、ステップ８０６、ステップ８０７、ステップ８０８、ステップ８０９乃至はステップ８０４、ステップ８０５、ステップ８０６、ステ

ップ８１０、ステップ８１１、ステップ８１２の繰り返しの回数は、（スカラー値dのビット長）−１回となるので、ステップ８０２での２倍算の計算量及びステップ８１６でのモンゴメリ型楕円曲線上の点への変換の計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）（ｋ−１）＋４Ｍ＋２Ｓとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ−３．６）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１４６８Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６００Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１６Ｍ＋２Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ−３．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５４）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１５２６Ｍとなる。楕円曲線とし

てワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第１０の実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d^W, Y_d^W, Z_d^W)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$d(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たに$P=(x, y)$とおく。高速スカラー倍計算部２０２は、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，x及びyを座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，x及びyよりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d^W, Y_d^W, Z_d^W)$の座標$X_d^W$、$Y_d^W$及び$Z_d^W$の復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d^W, Y_d^W, Z_d^W)$を計算結果として出力する。

次に図１８により、座標x，y，$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$が与えられた場合に$X_d^W$、$Y_d^W$、$Z_d^W$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び

$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でワイエルシュトラス型楕円曲線上で射影座標おいて完全な座標が与えられたスカラー倍点($X_d^W$, $Y_d^W$, $Z_d^W$)を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を($X_1$, $Y_1$, $Z_1$)でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を($x_d$, $y_d$)で、射影座標を($X_d$, $Y_d$, $Z_d$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d-1)Pのアフィン座標を($x_{d-1}$, $y_{d-1}$)で、射影座標を($X_{d-1}$, $Y_{d-1}$, $Z_{d-1}$)でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を($x_{d+1}$, $y_{d+1}$)で、射影座標を($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)でそれぞれ表す。

ステップ１８０１において$X_d \times x$が計算され、レジスタ$T_1$に格納される。ステップ１８０２において$T_1 - Z_d$が計算される。ここでレジスタ$T_1$には$X_d x$が格納されており、したがって$X_d x - Z_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１８０３において$Z_d \times x$が計算され、レジスタ$T_2$に格納される。ステップ１８０４において$X_d - T_2$が計算される。ここでレジスタ$T_2$には$Z_d x$が格納されており、したがって$X_d - xZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１８０５において$Z_{d+1} \times T_1$が計算される。ここでレジスタ$T_1$には$X_d x - Z_d$が格納されており、したがって$Z_{d+1}(X_d x - Z_d)$が計算される。その結果がレジスタ$T_3$に格納される。ステップ１８０６において$X_{d+1} \times T_2$が計算される。ここでレジスタ$T_2$には$X_d - xZ_d$が格納されており、したがって$X_{d+1}(X_d - xZ_d)$が計算される。その結果がレジスタ$T_4$に格納される。ステップ１８０７において$T_1$の２乗が計算される。ここでレジスタ$T_1$には$X_d x - Z_d$が格納されており、したがって$(X_d x - Z_d)^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１８０８において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$X_d - xZ_d$が格納されており、したがって$(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１８０９において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$(X_d - xZ_d)^2$が格納されており、したがって$Z_d(X_d - xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１８１０において$T_2 \times X_{d+1}$が計算される。ここでレジ

スタＴ$_2$には$Z_d(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}Z_d(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８１１においてＴ$_2$×$Z_{d+1}$が計算される。ここでレジスタＴ$_2$には$X_{d+1}Z_d(X_d-xZ_d)^2$が格納されており、したがって$Z_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８１２においてＴ$_2$×yが計算される。ここでレジスタＴ$_2$には$Z_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が格納されており、したがって$yZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８１３においてＴ$_2$×Bが計算される。ここでレジスタＴ$_2$には$yZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８１４においてＴ$_2$×$X_d$が計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d$が計算される。その結果がレジスタＴ$_5$に格納される。ステップ１８１５においてＴ$_2$×$Z_d$が計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2$が格納されており、したがって$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８１６においてＴ$_2$×sが計算される。ここでレジスタＴ$_2$には$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が格納されており、したがって$sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が計算される。その結果が$Z_dW$に格納される。ステップ１８１７において$\alpha\times Z_dW$が計算される。ここで$Z_dW$には$sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が格納されており、したがって$\alpha sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８１８においてＴ$_2$+Ｔ$_5$が計算される。ここでレジスタＴ$_2$には$\alpha sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$がレジスタＴ$_5$には$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d$がそれぞれ格納されており、したがって$\alpha sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d+ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d$が計算される。その結果が$X_d{}^W$に格納される。ステップ１８１９においてＴ$_3$+Ｔ$_4$が計算される。ここでレジスタＴ$_3$には$Z_{d+1}(X_dx-Z_d)$がレジスタＴ$_4$には$X_{d+1}(X_d-xZ_d)$が格納されており、したがって$Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ１８２０においてＴ$_3$−Ｔ$_4$が計

算される。ここでレジスタＴ$_3$には$Z_{d+1}(X_dx-Z_d)$がレジスタＴ$_4$には$X_{d+1}(X_d-xZ_d)$が格納されており、したがって$Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ１８２１においてＴ$_1$×Ｔ$_2$が計算される。ここでレジスタＴ$_1$には$(X_dx-Z_d)^2$がレジスタＴ$_2$には$Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)$が格納されており、したがって$\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ１８２２においてＴ$_1$×Ｔ$_3$が計算される。ここでレジスタＴ$_1$には$\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2$がレジスタＴ$_3$には$Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)$が格納されており、したがって$\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2$が計算される。その結果が$Y_d^W$に格納される。したがって$Y_d^W$には$\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2$が格納されている。$X_d^W$にはステップ１８１８において$ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d+\alpha sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が格納され、その後更新が行われないので、その値が保持されている。$X_d^W$にはステップ１８１６において$sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d$が格納され、その後更新が行われないので、その値が保持されている。その結果として、ワイエルシュトラス型楕円曲線における射影座標$(X_d^W, Y_d^W, Z_d^W)$の値が全て復元されている。

上記手順により与えられたx、y、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標$(X_d^W, Y_d^W, Z_d^W)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６、数７を得る。数６、数７の両辺を各々減算することにより、数８を得る。したがって、数９のようになる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、数１０を得る。モンゴメリ型楕円曲線の射影座標での加算公式は数１１、数１２である。ここで$X_m$及び$Z_m$はモンゴメリ型楕円曲線上の点Pのｍ倍点mPの射影座標におけるX座標及びZ座標、$X_n$及び$Z_n$はモンゴメリ型楕円曲線上の点Pのｎ倍点nPの射影座標におけるX

座標及びZ座標、$X_{m-n}$及び$Z_{m-n}$はモンゴメリ型楕円曲線上の点Pの(m-n)倍点(m-n)Pの射影座標におけるX座標及びZ座標、$X_{m+n}$及び$Z_{m+n}$はモンゴメリ型楕円曲線上の点Pの(m+n)倍点(m+n)Pの射影座標におけるX座標及びZ座標であり、m, nはm＞nをみたす正整数である。この式は$X_m/Z_m=x_m$、$X_n/Z_n=x_n$、$X_{m-n}/Z_{m-n}=x_{m-n}$が不変のとき、$X_{m+n}/Z_{m+n}=x_{m+n}$も不変となるので、射影座標での公式としてうまく働いている。他方、数１３、数１４とおくと、この式も$X_m/Z_m=x_m$、$X_n/Z_n=x_n$、$X_{m-n}/Z_{m-n}=x_{m-n}$が不変のとき、$X_{m+n}/Z_{m+n}=x_{m+n}$も不変となる。また、$X'_{m-n}/Z'_{m-n}=X_{m-n}/Z_{m-n}=x_{m-n}$をみたすので、$x_{m-n}$の射影座標として$X'_{m-n}, Z'_{m-n}$をとってよい。m=d, n=1として上記公式を用いて$y_d$の式より$X_{d-1}$及び$Z_{d-1}$を消去し、X1=x, Z1=1とおくことにより、数１５を得る。$x_d=X_d/Z_d$であるが、$y_d$の分母と通分することにより、数１６となる。その結果として、

$$Y'_d=\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2$$

…数４７

とし、

$$X'_d=ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d \quad \cdots 数４８$$

$$Z'_d=ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d \quad \cdots 数４９$$

とすると$(X'_d, Y'_d, Z'_d)=(X_d, Y_d, Z_d)$となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをsαとして、$Y_d^W=Y'_d$、$X_d^W=X'_d+\alpha Z_d^W$、及び$Z_d^W=sZ'_d$という関係がある。結果として次の式を得る。

$$Y_d^W=\{Z_{d+1}(X_dx-Z_d)+X_{d+1}(X_d-xZ_d)\}\{Z_{d+1}(X_dx-Z_d)-X_{d+1}(X_d-xZ_d)\}(X_dx-Z_d)^2$$

…数５０

$$X_d^W=ByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2X_d+\alpha Z_d^W \cdots 数５１$$

$$Z_d^W=sByZ_{d+1}X_{d+1}Z_d(X_d-xZ_d)^2Z_d \cdots 数５２$$

により更新すればよい。ここで、$X_d^W, Y_d^W, Z_d^W$は図１８の処理により与えら

れている。したがって、ワイエルシュトラス型楕円曲線における射影座標 $(X_d{}^W, Y_d{}^W, Z_d{}^W)$ の値が全て復元されていることになる。

上記手順はステップ１８０１、ステップ１８０３、ステップ１８０５、ステップ１８０６、ステップ１８０９、ステップ１８１０、ステップ１８１１、ステップ１８１２、ステップ１８１３、ステップ１８１４、ステップ１８１５、ステップ１８１６、ステップ１８１７、ステップ１８２１及びステップ１８２２において有限体上の乗算の計算量を必要とする。また、ステップ１８０７及びステップ１８０８において有限体上の２乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳとすると、上記手順は１５M＋２Ｓの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８Mと仮定すると座標復元の計算量は１６．６Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた $X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$ の値が計算できれば $X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$ の値が復元できる。また、ワイエルシュトラス型楕円曲線においてアフィン座標におけるスカラー倍点dPをdP=$(x_d{}^W, y_d{}^W)$ とすると、$x_d{}^W$、$y_d{}^W$ が上記計算式により与えられる値を取るように $X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$ の値を選択し、その値が計算できれば $X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$ が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタであるBの値やモンゴメリ型楕円曲線への変換パラメタsの値を小さくとることにより、ステップ１８１３乃至はステップ１８１６における乗算の計算量を削減することができる。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$ を出力するアルゴリズムについて説明する。

第１０実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第９実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及び

ワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記アルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１５Ｍ＋２Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ—３．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋１３）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１４８５Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第１１実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３が、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点

$(d-1)P=(X_{d-1},Y_{d-1},Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たに$P=(x,y)$とおく。高速スカラー倍計算部２０２は、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$，x及びyを座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$，x及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d,y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はワイエルシュトラス型楕円曲線上でアフィン座標において完全に座標が与えられたスカラー倍点$(x_d,y_d)$を計算結果として出力する。

次に図１９により、座標x，y，$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$が与えられた場合に$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d,Y_d,Z_d)$の座標うち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1},Y_{d+1},Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d-1)P=(X_{d-1},Y_{d-1},Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した$(x,y)$を入力し、以下の手順でワイエルシュトラス型楕円曲線上でアフィン座標おいて完全な座標が与えられたスカラー倍点$(x_d,y_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を$(x,y)$で、射影座標を$(X_1,Y_1,Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d^{Mon},y_d^{Mon})$で、射影座標を$(X_d,Y_d,Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点$(d-1)P$のアフィン座標を$(x_{d-1},y_{d-1})$で、射影座標を$(X_{d-1},Y_{d-1},Z_{d-1})$でそれぞれ表す。モンゴメリ型楕円曲線上の点$(d+1)P$のアフィン座標を$(x_{d+1},y_{d+1})$で、射影座標を$(X_{d+1},Y_{d+1},Z_{d+1})$でそれぞれ表す。

ステップ１９０１において$X_{d-1}\times Z_{d+1}$が計算され、レジスタ$T_1$に格納される。ステップ１９０２において$Z_{d-1}\times X_{d+1}$が計算され、レジスタ$T_2$に格

納される。ステップ１９０３において$T_1-T_2$が計算される。ここでレジスタ$T_1$には$X_{d-1}Z_{d+1}$がレジスタ$T_2$には$Z_{d-1}X_{d+1}$がそれぞれ格納されており、したがって$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１９０４において$Z_d\times X$が計算され、レジスタ$T_2$に格納される。ステップ１９０５において$X_d-T_2$が計算さる。ここでレジスタ$T_2$には$Z_d x$が格納されており、したがって$X_d-xZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９０６において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$X_d-xZ_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９０７において$T_1\times T_2$が計算される。ここでレジスタ$T_1$には$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$がレジスタ$T_2$には$(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が計算される。その結果がレジスタ$T_1$に格納される。ステップ１９０８において$4B\times y$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９０９において$T_2\times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$4By$が格納されており、したがって$4ByZ_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９１０において$T_2\times Z_{d-1}$が計算される。ここでレジスタ$T_2$には$4ByZ_{d+1}$が格納されており、したがって$4ByZ_{d-1}Z_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９１１において$T_2\times Z_d$が計算される。ここでレジスタ$T_2$には$4ByZ_{d-1}Z_{d+1}$が格納されており、したがって$4ByZ_{d-1}Z_{d+1}Z_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９１２において$T_2\times X_d$が計算される。ここでレジスタ$T_2$には$4ByZ_{d-1}Z_{d+1}Z_d$が格納されており、したがって$4ByZ_{d-1}Z_{d+1}Z_dX_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ１９１３において$T_2\times Z_d$が計算される。ここでレジスタ$T_2$には$4ByZ_{d-1}Z_{d+1}Z_d$が格納されており、したがって$4ByZ_{d-1}Z_{d+1}Z_dZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９１４において、$T_2\times s$が計算される。ここでレジスタ$T_2$には$4ByZ_{d-1}Z_{d+1}Z_dZ_d$が格納されており、したがって$4sByZ_{d-1}Z_{d+1}Z_dZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１９１５においてレジスタ$T_2$の逆元が計算される。

ここでレジスタ$T_2$には$4sByZ_{d-1}Z_{d+1}Z_dZ_d$が格納されており、したがって$1/4sByZ_{d-1}Z_{d+1}Z_dZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ１４１６において$T_2 \times T_3$が計算される。ここでレジスタ$T_2$には$1/4sByZ_{d-1}Z_{d+1}Z_dZ_d$がレジスタ$T_3$には$4ByZ_{d-1}Z_{d+1}Z_dX_d$がそれぞれ格納されており、したがって$(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d)$が計算される。その結果がレジスタ$T_3$に格納される。ステップ１９１７において$T_3+\alpha$が計算される。ここでレジスタ$T_3$には$(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d)$が格納されており、したがって$(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d)+\alpha$が計算される。その結果がレジスタ$x_d$に格納される。ステップ１９１８においてレジスタ$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$がレジスタ$T_2$には$1/4sByZ_{d-1}Z_{d+1}Z_dZ_d$がそれぞれ格納されており、したがって$(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2/4sByZ_{d-1}Z_{d+1}Z_d{}^2$が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には$(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2/4sByZ_{d-1}Z_{d+1}Z_d{}^2$が格納されている。レジスタ$x_d$にはステップ１９１７において$(4ByZ_{d-1}Z_{d+1}Z_dX_d)/(4sByZ_{d-1}Z_{d+1}Z_dZ_d)+\alpha$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標$(x_d, y_d)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数３８、数３９を得る。両辺を各々減算することにより、数４０を得る。したがって、数４１となる。ここで$x_d{}^{Mon}=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d=1}=X_{d=1}/Z_{d=1}$であり、この値を代入することにより射影座標の値へと変換すると、数４２を得る。$x_d{}^{Mon}=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d{}^{Mon}$の分母と通分することにより、数５３となる。

$x_d^{Mon}=(4ByZ_{d+1}Z_{d-1}Z_dX_d)/(4ByZ_{d+1}Z_{d-1}Z_dZ_d)$ …数５３

モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応

関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをs, αとして、$y_d = s^{-1} y_d^{Mon}$ 及び $x_d = s^{-1} x_d^{Mon} + \alpha$ の関係がある。結果として次の式を得る。

$y_d = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2 / 4sByZ_{d-1}Z_{d+1}Z_d^2$ …数５４

$x_d = (4ByZ_{d+1}Z_{d-1}Z_d X_d)/(4sByZ_{d+1}Z_{d-1}Z_d Z_d) + \alpha$ …数５５

ここで、$x_d$, $y_d$ は図１９により与えられる。したがって、ワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標($x_d$, $y_d$)における値が全て復元されることになる。

上記手順はステップ１９０１、ステップ１９０２、ステップ１９０４、ステップ１９０７、ステップ１９０８、ステップ１９０９、ステップ１９１０、ステップ１９１１、ステップ１９１２、ステップ１９１３、ステップ１９１４、ステップ１９１６及びステップ１９１８において有限体上の乗算の計算量を必要とする。また、ステップ１９０６において有限体上の２乗算の計算量を必要とする。また、ステップ１９１４において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１３M＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M、Ｉ＝４０Mと仮定すると座標復元の計算量は５３．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$, $y_d$の値が計算できれば$x_d$, $y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタであるBの値乃至はモンゴメリ型楕円曲線への変換パラメタであるsの値をを小さくとること

により、ステップ１９０８乃至はステップ１９１４における乗算の計算量を削減することができる。

次に図１０により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d+1}$，$Z_{d-1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP=($X_d$, $Y_d$, $Z_d$)のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P=($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点(d-1)P=($X_{d-1}$, $Y_{d-1}$, $Z_{d-1}$)のうち$X_{d-1}$及び$Z_{d-1}$を出力する。ステップ１０１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ１００１として、変数Ｉに初期値１を代入する。ステップ１００２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(x, y, 1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ１００３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ１００２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ１００４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップm＝ｄとなり、１０１４へ行く。一致しなければステップ１００５へ行く。ステップ１００５として、変数Ｉを１増加させる。ステップ１００６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ１００７へ行く。そのビットの値が１であればステップ１０１０へ行く。ステップ１００７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ１００８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ１００８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍

算２(mP)を行ない、点2mPを計算する。その後ステップ１００９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ１００９として、ステップ１００８で求めた点2mPとステップ１００７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ１００４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ１０１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ１０１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ１０１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ１０１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ１０１２として、ステップ１０１０で求めた点(2m+１)Pとステップ１０１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ１００４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ１０１４として、射影座標で表された点の組(mP, (m+１)P)から、点(m−1)Pの射影座標におけるX座標$X_{m-1}$及びZ座標を$Z_{m-1}$求め、それぞれ$X_{d-1}$及び$Z_{d-1}$とする。その後ステップ１０１３へ行く。ステップ１０１３として、射影座標で表された点mP＝$(X_m, Y_m, Z_m)$より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$として、射影座標で表された点(m+1)P＝$(X_{m+1}, Y_{m+1}, Z_{m+1})$より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$として、$X_{d-1}$及び$Z_{d-1}$と共に出力する。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。また上記手順により、mとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

また、ステップ１０１４において(m-1)Pを求める際に、数１３、数１４の公式より求めてもよいし、mが奇数であれば、((m-1)/2)Pの値をステップ１０１２の

段階で別に保持しておき、その値からモンゴメリ型楕円曲線の２倍の公式より、(m-1)Pを求めてもよい。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1=1$とることにより３Ｍ＋２Ｓとなる。ここでＭは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ１００７において加算の計算量、ステップ１００８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ１０１０において加算の計算量、ステップ１０１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ１００４、ステップ１００５、ステップ１００６、ステップ１００７、ステップ１００８、ステップ１００９乃至はステップ１００４、ステップ１００５、ステップ１００６、ステップ１０１０、ステップ１０１１、ステップ１０１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ１００２での２倍算の計算量とステップ１０１４での(m-1)Pの計算に必要な計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋Ｍとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋３）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１４７５Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６００Ｍと

なる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Y_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１３M＋S＋Iであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２k＋１）Mとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。I＝４０M、S＝０．８Mと仮定すると、この計算量はおおよそ（９．２k＋５６．８）Mと見積もることができる。例えばスカラー値dが１６０ビット（k＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１５２９Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Mであり、これと比べて必要となる計算量は削減されている。

第１２実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いる。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d^W, Y_d^W, Z_d^W)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点

(d-1)P=$(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d=1}$及び$Z_{d-1}$を計算し、射影座標で表された入力されたワイエルシュトラス型楕円曲線上の点P=(x, y)と共にその情報を座標復元部２０３に与える。座標変換部２０３は与えられた座標の値$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$，x及びyよりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点dP=$(X_d{}^W, Y_d{}^W, Z_d{}^W)$の座標$X_d{}^W$、$Y_d{}^W$及び$Z_d{}^W$の復元を行なう。スカラー倍計算部１０３はワイエルシュトラス型楕円曲線上で座標射影座標において完全に座標が与えられたスカラー倍点$(X_d{}^W, Y_d{}^W, Z_d{}^W)$を計算結果として出力する。

次に図２０により、座標x，y，$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$が与えられた場合に$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP=$(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P=$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、射影座標で表されたモンゴメリ型楕円曲線上の点(d-1)P=$(X_{d-1}, Y_{d-1}, Z_{d-1})$の座標のうち$X_{d-1}$及び$Z_{d-1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを射影座標で表した(x, y)を入力し、以下の手順でワイエルシュトラス型楕円曲線上で射影座標おいて完全な座標が与えられたスカラー倍点$(X_d{}^W, Y_d{}^W, Z_d{}^W)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d-1)Pのアフィン座標を$(x_{d-1}, y_{d-1})$で、射影座標を$(X_{d-1}, Y_{d-1}, Z_{d-1})$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ２００１において$X_{d-1} \times Z_{d+1}$が計算され、レジスタ$T_1$に格納される。ステップ２００２において$Z_{d-1} \times X_{d+1}$が計算され、レジスタ$T_2$に格納される。ステップ２００３において$T_1 - T_2$が計算される。ここでレジスタ

Ｔ$_1$には$X_{d-1}Z_{d+1}$がレジスタＴ$_2$には$Z_{d-1}X_{d+1}$がそれぞれ格納されており、したがって$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ２００４において$Z_d\times x$が計算され、レジスタＴ$_2$に格納される。ステップ２００５において$X_d-T_2$が計算さる。ここでレジスタＴ$_2$には$Z_dx$が格納されており、したがって$X_d-xZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２００６においてＴ$_2$の２乗が計算される。ここでレジスタＴ$_2$には$X_d-xZ_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２００７において$T_1\times T_2$が計算される。ここでレジスタＴ$_1$には$X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1}$がレジスタＴ$_2$には$(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が計算される。その結果が$Y_d^W$に格納される。ステップ２００８において$4B\times y$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２００９において$T_2\times Z_{d+1}$が計算される。ここでレジスタＴ$_2$には$4By$が格納されており、したがって$4ByZ_{d+1}$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２０１０において$T_2\times Z_{d-1}$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２０１１において$T_2\times Z_d$が計算される。ここでレジスタＴ$_2$には$4yZ_{d+1}Z_{d-1}$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２０１２において$T_2\times X_d$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dX_d$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ２０１３において$T_2\times Z_d$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}Z_{d-1}Z_d$が格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２０１４において$T_2\times s$が計算される。ここでレジスタＴ$_2$には$4ByZ_{d+1}Z_{d-1}Z_dZ_d$が格納されており、したがって$4sByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタ$Z_d^W$格納される。ステップ２０１５において$\alpha\times Z_d^W$が計算される。ここでレジスタ$Z_d^W$には$4sByZ_{d+1}Z_{d-1}Z_dZ_d$が格納されており、したがって

$4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ２０１６においてＴ$_1$+Ｔ$_2$が計算される。ここでレジスタＴ$_1$には$4ByZ_{d+1}Z_{d-1}Z_dX_d$がレジスタＴ$_2$には$4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$がそれぞれ格納されており、したがって$4ByZ_{d+1}Z_{d-1}Z_dX_d+4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$が計算される。その結果がレジスタ$X_d{}^W$に格納される。したがってレジスタ$X_d{}^W$には$4ByZ_{d+1}Z_{d-1}Z_dX_d+4\alpha sByZ_{d+1}Z_{d-1}Z_dZ_d$が格納されている。レジスタ$Y_d{}^W$にはステップ２００７において$(X_d-xZ_d)^2(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})$が格納され、その後更新が行なわれないので、その値が保持されている。レジスタ$Z_d{}^W$にはステップ２０１４において$4sByZ_{d+1}Z_{d-1}Z_dZ_d$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられたｘ、ｙ、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、$X_{d-1}$、$Z_{d-1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標$(X_d{}^W, Y_d{}^W, Z_d{}^W)$における値が全て復元される理由は以下の通りである。尚、点(d+1)Pは点dPに点Pを加算した点であり、点(d-1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６、数７を得る。両辺を各々減算することにより、数８を得る。したがって、数９となる。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$、$x_{d-1}=X_{d-1}/Z_{d-1}$であり、この値を代入することにより射影座標の値へと変換すると、数１０を得る。

$x_d=X_d/Z_d$であるが、$y_d$の分母と通分することにより、数２０となる。その結果として、

$$Y'_d=(X_{d-1}Z_{d+1}-Z_{d-1}X_{d+1})(X_d-Z_dx)^2 \cdots \text{数５６}$$

とし、

$$X'_d=4ByZ_{d+1}Z_{d-1}Z_dX_d \cdots \text{数５７}$$

$$Z'_d=4ByZ_{d+1}Z_{d-1}Z_dZ_d \cdots \text{数５８}$$

とすると$(X'_d, Y'_d, Z'_d)=(X_d, X_d, X_d)$となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751

(2000) pp. 238-257 に記載されている。それによると、変換パラメタをs, $\alpha$として、$Y_d{}^W$ = $Y'_d$、$X_d{}^W = X'_d + \alpha Z_d{}^W$及び$Z_d{}^W = sZ'_d$の関係がある。結果として次の式を得る。

$Y_d^W = (X_{d-1}Z_{d+1} - Z_{d-1}X_{d+1})(X_d - Z_d x)^2$ …数５９

$X_d^W = 4ByZ_{d+1}Z_{d-1}Z_d X_d + \alpha 4sByZ_{d+1}Z_{d-1}Z_d Z_d$ …数６０

$Z_d^W = 4sByZ_{d+1}Z_{d-1}Z_d Z_d$ …数６１

となる。ここで、$X_d{}^W$, $Y_d{}^W$, $Z_d{}^W$は図２０により与えられる。したがって、ワイエルシュトラス型楕円曲線における射影座標($X_d{}^W$, $Y_d{}^W$, $Z_d{}^W$)の値が全て復元されていることになる。

上記手順はステップ２００１、ステップ２００２、ステップ２００４、ステップ２００７、ステップ２００８、ステップ２００９、ステップ２０１０、ステップ２０１１、ステップ２０１２、ステップ２０１３、ステップ２０１４及びステップ２０１５において有限体上の乗算の計算量を必要とする。また、ステップ２００６において有限体上の２乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳとすると、上記手順は１２Ｍ＋Ｓの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８Ｍと仮定すると座標復元の計算量は１２．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$の値が計算できれば$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$の値が復元できる。また、ワイエルシュトラス型楕円曲線においてアフィン座標におけるスカラー倍点dPをdP=($x_d{}^W$、,$y_d{}^W$)とすると、$x_d{}^W$、$y_d{}^W$が上記計算式により与えられる値を取るように$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$の値を選択し、その値が計算できれば$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBやモンゴメリ型楕円曲線への変換パラ

メタであるｓの値を小さくとることにより、ステップ２００８乃至はステップ２０１４における乗算の計算量を削減することができる。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムについて説明する。

第１２実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第１１実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，$X_{d-1}$，$Z_{d-1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１２Ｍ＋Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋１）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋１３．８）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１４８６Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第１３実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３が、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点

$(x_d{}^W, y_d{}^W)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d-1)P=(x_{d-1}, y_{d-1})$の座標のうち$x_{d-1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$x_d$、$x_{d+1}$、$x_{d-1}$、x及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d{}^W, y_d{}^W)$の座標$y_d{}^W$の復元を行なう。スカラー倍計算部１０３はワイエルシュトラス型楕円曲線上でアフィン座標において完全に座標が与えられたスカラー倍点$(x_d{}^W, y_d{}^W)$を計算結果として出力する。

次に図２１により、座標x、y、$x_d$、$x_{d+1}$、$x_{d-1}$が与えられた場合に、$x_d{}^W$、$y_d{}^W$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d-1)P=(x_{d-1}, y_{d-1})$の座標のうち$x_{d-1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した$(x, y)$を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点$(x_d{}^W, y_d{}^W)$を出力する。

ステップ２１０１において$x_d-x$が計算され、レジスタ$T_1$に格納される。ステップ２１０２において$T_1$の２乗すなわち$(x_d-x)^2$が計算され、レジスタ$T_1$に格納される。ステップ２１０３において$x_{d-1}-x_{d+1}$が計算され、レジスタ$T_2$に格納される。ステップ２１０４において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(x_d-x)^2$がレジスタ$T_2$には$x_{d-1}-x_{d+1}$がそれぞれ格納されており、したがって$(x_d-x)^2(x_{d-1}-x_{d+1})$が計算される。その結果

がレジスタ$T_1$に格納される。ステップ２１０５において4B×yが計算され、レジスタ$T_2$に格納される。ステップ２１０６において$T_2$の逆元が計算される。ここでレジスタ$T_2$には4Byが格納されており、したがって1/4Byが計算される。その結果がレジスタ$T_2$に格納される。ステップ２１０７において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(x_d - x)^2 (x_{d-1} - x_{d+1})$がレジスタ$T_2$には1/4Byがそれぞれ格納されており、したがって$(x_d - x)^2 (x_{d-1} - x_{d+1})/4By$が計算される。その結果がレジスタ$T_1$に格納される。ステップ２１０８において$T_1 \times s^{-1}$が計算される。ここでレジスタ$T_1$には$(x_d - x)^2 (x_{d-1} - x_{d+1})/4By$が格納されており、したがって$(x_d - x)^2 (x_{d-1} - x_{d+1})/4sBy$が計算される。その結果がレジスタ$y_d{}^W$に格納される。尚、sはあらかじめ与えられている値であり、したがってあらかじめ$s^{-1}$を計算できる。ステップ２１０９において$x_d \times s^{-1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ２１１０において$T_1 + \alpha$が計算される。ここでレジスタ$T_1$には$s^{-1} x_d$が格納されており、したがって$s^{-1} x_d + \alpha$が計算される。その結果がレジスタ$x_d{}^W$に格納される。したがってレジスタ$x_d{}^W$には$s^{-1} x_d + \alpha$が格納されている。レジスタ$y_d{}^W$はステップ２１０８において$(x_d - x)^2 (x_{d-1} - x_{d+1})/4sBy$が格納され、その後更新されないので、その値が保持されている。

上記手順によりスカラー倍点のy座標$y_d$が復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。点(d-1)Pは点dPから点Pを減算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６、数７を得る。両辺を各々減算することにより、数８を得る。したがって、数９となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをs, αとして、$y_d{}^W = s^{-1} y_d$及び$x_d{}^W = s^{-1} x_d + \alpha$の関係がある。結果として次の式を得る。

$$y_d^W = (x_{d-1} - x_{d+1})(x_d - x)^2 / 4sBy \qquad \cdots 数６２$$

$$x_d^W = s^{-1} x_d + \alpha \qquad \cdots 数６３$$

ここで、$x_d^W$, $y_d^W$は図２１により与えられる。したがって、アフィン座標($x_d^W$, $y_d^W$)の値は全て復元されていることになる。

上記手順はステップ２１０４、ステップ２１０５、ステップ２１０７、ステップ２１０８及びステップ２１０９において有限体上の乗算の計算量を必要とする。また、ステップ２１０２において有限体上の２乗算の計算量を必要とする。さらにステップ２１０６において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ、有限体上の逆元演算の計算量をＩとすると、上記手順は５Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M及びＩ＝４０Mと仮定すると座標復元の計算量は４５．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば$y_d^W$の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBやモンゴメリ型楕円曲線への変換パラメタsの値を小さくとることにより、ステップ２１０５、ステップ２１０８乃至はステップ２１０９における乗算の計算量を削減することができる。

次に図２４により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$, $x_{d+1}$, $x_{d=1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP=($x_d$, $y_d$)のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d+1)P=($x_{d+1}$, $y_{d+1}$)のうち$x_{d+1}$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d−1)P=($x_{d-1}$, $y_{d-1}$)のうち$x_{d-1}$を出力する。ステップ２４１６として、与えられ

たワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ２４０１として、変数Ｉに初期値１を代入する。ステップ２４０２として、点Pの２倍点2Pを計算する。ここで点Pは射影座標において(x, y, 1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ２４０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ２４０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ２４０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればｍ＝ｄとなり、ステップ２４１４へ行く。一致しなければステップ２４０５へ行く。ステップ２４０５として、変数Ｉを１増加させる。ステップ２４０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ２４０７へ行く。そのビットの値が１であればステップ２４１０へ行く。ステップ２４０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ２４０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ２４０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算2(mP)を行ない、点2mPを計算する。その後ステップ２４０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ２４０９として、ステップ２４０８で求めた点2mPとステップ２４０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ２４０４へ戻る。ここで、点2mP、点(2m+1)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ２４１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ２４１１へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ２４１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステ

ップ２４１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ２４１２として、ステップ２４１０で求めた点(2m+１)Pとステップ２４１１で求めた点(2m+2)Pを点の組((2m+１)P, (2m+2)P)として、点の組(mP, (m+1)Pの代わりに格納する。その後ステップ２４０４へ戻る。ここで、点(2m+１)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ２４１４として、射影座標で表された点の組(mP, (m+１)P)から、点(m−1)Pの射影座標におけるX座標$X_{m-1}$及びZ座標$Z_{m-1}$を求め、それぞれ$X_{d-1}$及び$Z_{d-1}$とする。その後ステップ２４１５へ行く。ステップ２４１５として、射影座標で表された点mP=($X_m$, $Y_m$, $Z_m$)より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$とし、射影座標で表された点(m+1)P＝($X_{m+1}$, $Y_{m+1}$, $Z_{m+1}$)より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$とする。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。$X_{d-1}$，$Z_{d+1}$，$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$より、数２４、数２５、数２６として$x_{d-1}$，$x_d$，$x_{d+1}$を求める。その後ステップ２４１３へ行く。ステップ２４１３として、$x_{d-1}$，$x_d$，$x_{d+1}$を出力する。上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。またステップ２４１４において(m-1)Pを求める際に、数１３、数１４の公式により求めてもよいし、ｍが奇数であれば、((m−1)/2)Pの値をステップ２４１２の段階で別に保持しておき、その値からモンゴメリ型楕円曲線の２倍算の公式より、(m-1)Pを求めてもよい。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1$=1ととることにより３Ｍ＋２Ｓとなる。ここでＭは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ２４０７において加算の計算量、ステップ２４０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ２４１０において加算の計算量、ステップ２４１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの

計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ２４０４、ステップ２４０５、ステップ２４０６、ステップ２４０７、ステップ２４０８、ステップ２４０９乃至はステップ２４０４、ステップ２４０５、ステップ２４０６、ステップ２４１０、ステップ２４１１、ステップ２４１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ２４０２での２倍算の計算量、ステップ２４１４での(m-1)Pの計算に必要な計算量及びステップ２４１５でのアフィン座標への変換の計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋１１Ｍ＋Ｉとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度、計算量Ｉは Ｉ＝４０Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋５１）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１５２３Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６４０Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_{d-1}$, $x_d$, $x_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

第１４の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Ｐから、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点（$x_d$, $y_d$）を計算し出力するものであ

る。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値ｄと与えられたモンゴメリ型楕円曲線上の点Ｐからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$ の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点P＝（ｘ，ｙ）と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、ｘ及びｙよりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図３４により、座標x, y, $X_d, Z_d, X_{d+1}, Z_{d+1}$が与えられた場合に$x_d, y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標うち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ３４０１において$x \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ３４０２において$X_d+T_1$が計算される。ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d+X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３４０３において$X_d-T_1$が計算され、ここでレジスタ

$T_1$にはx$Z_d$ が格納されており、したがってx$Z_d$-$X_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３４０４においてレジスタ$T_3$の２乗が計算される。ここでレジスタ$T_3$にはx$Z_d$-$X_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３４０５において$T_3 \times X_{d+1}$が計算される。ここでレジスタ$T_3$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３４０６において$2A \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ３４０７において$T_2+T_1$が計算される。ここでレジスタ$T_2$には$xZ_d+X_d$がレジスタ$T_1$には$2AZ_d$がそれぞれ格納されており、したがって$xZ_d+X_d+2AZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３４０８において$x \times X_d$が計算され、レジスタ$T_4$に格納される。ステップ３４０９において$T_4+Z_d$が計算される。ここでレジスタ$T_4$には$xX_d$が格納されており、したがって$xX_d+Z_d$が計算される。その結果がレジスタ$T_4$に格納される。ステップ３４１０において$T_2 \times T_4$が計算される。ここでレジスタ$T_2$には$xZ_d+X_d+2AZ_d$がレジスタ$T_4$には$xX_d+Z_d$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３４１１において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2AZ_d$が格納されており、したがって$2AZ_d{}^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３４１２において$T_2-T_1$が計算される。ここでレジスタ$T_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$がここでレジスタ$T_1$には$2AZ_d{}^2$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３４１３において$T_2 \times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2$が格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３４１４において$T_2-T_3$が計算される。ここでレジスタ$T_2$には$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)$がレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)\ (xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_2$に格納され

る。ステップ３４１５において$2B \times y$が計算され、レジスタ$T_1$に格納される。ステップ３４１６において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2By$が格納されており、したがって$2ByZ_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３４１７において$T_1 \times Z_{d+1}$が計算される。ここでレジスタ$T_1$には$2ByZ_d$が格納されており、したがって$2ByZ_d Z_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３４１８において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2ByZ_d Z_{d+1}$が格納されており、したがって$2ByZ_d Z_{d+1} Z_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３４１９においてレジスタ$T_3$の逆元が計算される。ここでレジスタ$T_3$には$2ByZ_d Z_{d+1} Z_d$が格納されており、したがって$1/2ByZ_d Z_{d+1} Z_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３４２０において$T_2 \times T_3$が計算される。ここでレジスタ$T_2$には$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2$がレジスタ$T_3$には$1/2ByZ_d Z_{d+1} Z_d$がそれぞれ格納されており、したがって$\{Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2\}/2ByZ_d Z_{d+1}\ Z_d$が計算される。その結果がレジスタ$y_d$に格納される。ステップ３４２１において$T_1 \times X_d$が計算される。ここでレジスタ$T_1$には$2ByZ_d Z_{d+1}$が格納されており、したがって$2ByZ_d\ Z_{d+1} X_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３４２２において$T_1 \times T_3$が計算される。ここでレジスタ$T_1$には$2ByZ_d Z_{d+1} X_d$がレジスタ$T_3$には$1/2ByZ_d Z_{d+1} Z_d$がそれぞれ格納されており、したがって$2ByZ_d Z_{d+1} X_d\ /2ByZ_d Z_{d+1} Z_d (=X_d/Z_d)$が計算される。その結果が$x_d$に格納される。$y_d$にはステップ３４２０において$\{Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2\}/2By\ Z_d Z_{d+1} Z_d$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により座標復元部２０３へ与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からモンゴメリ型楕円曲線におけるスカラー倍点のアフィン座標$(x_d, y_d)$における値が全て復元される理由は以下の通りである。尚、点$(d+1)P$は点$dP$に点$P$を加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６を得る。点P及び点dPはモンゴメリ型楕円曲線上の点

であるので、$By_d^2=x_d^3+Ax_d^2+x_d$ 及び $By^2=x^3+Ax^2+x$ をみたす。数６に代入し、$By_d^2$ 及び $By^2$ を消去し、式を整理すると、

$$y_d=\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/(2By) \quad \cdots 数64$$

を得る。ここで $x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d=\{Z_{d+1}\left((X_d x+Z_d)(X_d+xZ_d+2AZ_d)-2AZ_d^2\right)-(X_d-xZ_d)^2 X_{d+1}\}/(2ByZ_d Z_{d+1} Z_d) \quad \cdots 数65$$

$x_d=X_d/Z_d$ であるが、逆元演算の回数を減らす目的で $y_d$ の分母と通分することにより、

$$X_d=(2ByZ_d Z_{d+1} X_d)/(2ByZ_d Z_{d+1} Z_d) \quad \cdots 数66$$

となる。ここで、$x_d$，$y_d$ は図３４の処理により与えられている。したがって、アフィン座標 $(x_d, y_d)$ の値が全て復元されていることになる。

上記手順はステップ３４０１、ステップ３４０５、ステップ３４０６、ステップ３４０８、ステップ３４１０、ステップ３４１１、ステップ３４１３、ステップ３４１５、ステップ３４１６、ステップ３４１７、ステップ３４１８、ステップ３４２０、ステップ３４２１及びステップ３４２２において有限体上の乗算の計算量を必要とする。また、ステップ３４０４において有限体上の２乗算の計算量を必要とする。また、ステップ３４１９において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１４Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値 $d$ が１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００Ｍ弱と見積もられる。Ｓ＝０．８Ｍ、Ｉ＝４０Ｍと仮定すると座標復元の計算量は５４．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた $x_d$，$y_d$ の値が計算できれば $x_d$，$y_d$ の値が復元できる。その場合においては一般的に復元に

必要となる計算量が増大する。また、楕円曲線のパラメタであるA乃至はBの値を小さくとることにより、ステップ３４０６乃至はステップ３４１５における乗算の計算量を削減することができる。

次にスカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d, Z_d, X_{d+1}, Z_{d+1}$を出力する高速スカラー倍計算部の処理を説明する。

第１４実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第１実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記アルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１４Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ－４．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５０）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１５２２Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第１５の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算し出力するものである。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０

２は受け取ったスカラー値dと与えられたモンゴメリ型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、x及びyよりモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標$X_d, Y_d$及び$Z_d$の復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算結果として出力する。

次に図３５により、座標x、y $X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$が与えられた場合に$X_d$、$Y_d$、$Z_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した$(x, y)$を入力し、以下の手順で射影座標おいて完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を$(x, y)$で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ３５０１において$x \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ３５０２において$X_d+T_1$が計算される。ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d+X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３５０３において$X_d-T_1$が計算され、ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d-X_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３５０４においてレジスタ$T_3$の２乗が計

算される。ここでレジスタ$T_3$には$xZ_d-X_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３５０５において$T_3 \times X_{d+1}$が計算される。ここでレジスタ$T_3$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３５０６において$2A \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ３５０７において$T_2+T_1$が計算される。ここでレジスタ$T_2$には$xZ_d+X_d$がレジスタ$T_1$には$2AZ_d$がそれぞれ格納されており、したがって$xZ_d+X_d+2AZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３５０８において$x \times X_d$が計算され、レジスタ$T_4$に格納される。ステップ３５０９において$T_4+Z_d$が計算される。ここでレジスタ$T_4$には$xX_d$が格納されており、したがって$xX_d+Z_d$が計算される。その結果がレジスタ$T_4$に格納される。ステップ３５１０において$T_2 \times T_4$が計算される。ここでレジスタ$T_2$には$xZ_d+X_d+2AZ_d$がレジスタ$T_4$には$xX_d+Z_d$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３５１１において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2AZ_d$が格納されており、したがって$2AZ_d^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３５１２において$T_2-T_1$が計算される。ここでレジスタ$T_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$がここでレジスタ$T_1$には$2AZ_d^2$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３５１３において$T_2 \times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^2$が格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^2)$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３５１４において$T_2-T_3$が計算される。ここでレジスタ$T_2$には$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^2)$がレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^2)-X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$Y_d$に格納される。ステップ３５１５において$2B \times y$が計算され、レジスタ$T_1$に格納される。ステップ３５１６において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2By$

が格納されており、したがって$2ByZ_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３５１７において$T_1 \times Z_{d+1}$が計算される。ここでレジスタ$T_1$には$2ByZ_d$が格納されており、したがって$2ByZ_dZ_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３５１８において$T_1 \times X_d$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}$が格納されており、したがって$2ByZ_dZ_{d+1}X_d$が計算される。その結果がレジスタ$X_d$に格納される。ステップ３５１９において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}$が格納されており、したがって$2ByZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$Z_d$に格納される。$X_d$にはステップ３５１８において$2ByZ_dZ_{d+1}X_d$が格納され、その後更新が行なわれないので、その値が保持されている。$Y_d$にはステップ３５１４において$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられたx、y、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からスカラー倍点の射影座標$(X_d, Y_d, Z_d)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、次の数６を得る。点P及び点dPはモンゴメリ型楕円曲線上の点であるので、$By_d{}^2=x_d{}^3+Ax_d{}^2+x_d$及び$By^2=x^3+Ax^2+x$をみたす。数６に代入し、$By_d{}^2$及び$By^2$を消去し、式を整理すると、数６４を得る。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$であり、この値を代入することにより射影座標の値へと変換すると、数６５を得る。$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、数６６となる。その結果として、

$$Y_d=Z_{d+1}[(X_d+xZ_d+2AZ_d)(X_dx+Z_d)-2AZ_d^2]-(X_d-xZ_d)^2X_{d+1} \quad \cdots 数６７$$

とし、$X_d$及び$Z_d$をそれぞれ

$$2ByZ_dZ_{d+1}X_d \quad \cdots 数６８$$

$$2ByZ_dZ_{d+1}X_d \quad \cdots 数６９$$

により更新すればよい。ここで、$X_d$，$Y_d$，$Z_d$は図３５の処理により与えられている。したがって、射影座標$(X_d, Y_d, Z_d)$の値が全て復元されていることになる。

上記手順はステップ３５０１、ステップ３５０５、ステップ３５０６、ステッ

プ３５０８、ステップ３５１０、ステップ３５１１、ステップ３５１３、ステップ３５１５、ステップ３５１６、ステップ３５１７、ステップ３５１８及びステップ３５１９において有限体上の乗算の計算量を必要とする。また、ステップ３５０４において有限体上の２乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳとすると、上記手順は１２Ｍ＋Ｓの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８Ｍと仮定すると座標復元の計算量は１２．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d$、$Y_d$、$Z_d$の値が計算できれば$X_d$、$Y_d$、$Z_d$の値が復元できる。また、$x_d$、$y_d$が上記計算式により与えられる値を取るように$X_d$、$Y_d$、$Z_d$の値を選択し、その値が計算できれば$X_d$、$Y_d$、$Z_d$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるA乃至はBの値を小さくとることにより、ステップ３５０６乃至はステップ３５１５における乗算の計算量を削減することができる。

次に、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムについて説明する。

第１５実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第１実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記アルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量

は１２Ｍ＋Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ—４．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋８）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１４８０Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第１６の実施例は、スカラー倍計算部１０３がスカラー値d及びモンゴメリ型楕円曲線上の点Pから、モンゴメリ型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力する。スカラー値d及びモンゴメリ型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたモンゴメリ型楕円曲線上の点Pからモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$x_d$、$x_{d+1}$、x及びyよりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図３６により、座標x、y、$x_d$、$x_{d+1}$が与えられた場合に、$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴ

メリ型楕円曲線上の点$(_{d+1})$P＝$(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した$(x, y)$を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。

ステップ３６０１において$x_d \times x$が計算され、レジスタ$T_1$に格納される。ステップ３６０２において$T_1+1$が計算される。ここでレジスタ$T_1$には$x_d x$が格納されており、したがって$x_d x+1$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３６０３において$x_d+x$が計算され、レジスタ$T_2$に格納される。ステップ３６０４において$T_2+2A$が計算される。ここでレジスタ$T_2$には$x_d+x$が格納されており、したがって$x_d+x+2A$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３６０５において$T_1 \times T_1$が計算される。ここでレジスタ$T_1$には$x_d x+1$がレジスタ$T_2$には$x_d+x+2A$がそれぞれ格納されており、したがって$(x_d x+1)(x_d+x+2A)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３６０６において$T_1-2A$が計算される。ここでレジスタ$T_1$には$(x_d x+1)(x_d+x+2A)$が格納されており、したがって$(x_d x+1)(x_d+x+2A)-2A$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３６０７において$x_d-x$が計算され、レジスタ$T_1$に格納される。ステップ３６０８において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$x_d-x$が格納されており、したがって$(x_d-x)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３６０９において$T_2 \times x_{d+1}$が計算される。ここでレジスタ$T_2$には$(x_d-x)^2$が格納されており、したがって$(x_d-x)^2 x_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３６１０において$T_1-T_2$が計算される。ここでレジスタ$T_1$には$(x_d x+1)(x_d+x+2A)-2A$がレジスタ$T_2$には$(x_d-x)^2 x_{d+1}$がそれぞれ格納されており、したがって$(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３６１１において$2B \times y$が計算され、レジスタ$T_2$に格納される。ステップ３６１２において$T_2$の逆元が計算される。ここでレジスタ$T_2$には$2By$が格納されており、したがって$1/2By$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３６１３において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には

$(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$がレジスタ$T_2$には1/2Byがそれぞれ格納されており、したがって$(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}/2By$が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には$(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}/2By$が格納されている。レジスタ$x_d$は全く更新されないので入力された値が保持されている。

上記手順によりスカラー倍点のy座標$y_d$が復元される理由は以下の通りである。尚、点$(d+1)$Pは点dPに点Pを加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６を得る。点P及び点dPはモンゴメリ型楕円曲線上の点であるので、$By_d^2=x_d^3+Ax_d^2+x_d$及び$By^2=x^3+Ax^2+x$をみたす。数６に代入し、$By_d^2$及び$By^2$を消去し、式を整理すると、数６４を得る。ここで、$x_d$，$y_d$は図３６の処理により与えられる。したがって、アフィン座標$(x_d, y_d)$の値は全て復元されたことになる。

上記手順はステップ３６０１、ステップ３６０５、ステップ３６０９、ステップ３６１１及びステップ３６１３において有限体上の乗算の計算量を必要とする。また、ステップ３６０８において有限体上の２乗算の計算量を必要とする。さらにステップ３６１２において有限体上の逆元演算の計算量を必要とする。有限体上の減算の計算量は、有限体上の乗算の計算量、２乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ、有限体上の逆元演算の計算量をＩとすると、上記手順は５Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８Ｍ及びＩ＝４０Ｍと仮定すると座標復元の計算量は４５．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば$y_d$の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメタであるBの値を小さくとることにより、ステップ２６０５における乗算の計算量を削減することができる。

次に図４３により、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$x_d$、$x_{d+1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(x_{d+1}, y_{d+1})$のうち$x_{d+1}$を出力する。ステップ４３０１として、変数Ｉに初期値１を代入する。ステップ４３０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(x，y,1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ４３０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ４３０２で求めた点2Pを、点の組(P,2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ４３０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ４３１５へ行く。一致しなければステップ４３０５へ行く。ステップ４３０５として、変数Ｉを１増加させる。ステップ４３０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ４３０７へ行く。そのビットの値が１であればステップ４３１０へ行く。ステップ４３０７として、射影座標により表された点の組(mP,(m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ４３０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４３０８として、射影座標により表された点の組(mP,(m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ４３０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４３０９として、ステップ４３０８で求めた点2mPとステップ４３０７で求めた点(2m+１)Pを点の組(2mP,（2m+１)P)として、点の組(mP,(m+１)P)の代わりに格納する。その後ステップ４３０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ４３１０として、射影座標により表された点の組(mP,(m+１)P)から点mPと点

(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ４３１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４３１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ４３１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４３１２として、ステップ４３１０で求めた点(2m+１)Pとステップ４３１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ４３０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ４３１５として、射影座標で表された点$mP=(X_m, Y_m, Z_m)$より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$とし、射影座標で表された点$(m+1)P=(X_{m+1}+1, Y_{m+1}, Z_{m+1})$より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$とする。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$より、$x_d=X_d Z_{d+1}/Z_d Z_{d+1}$，$x_{d+1}=Z_d X_{d+1}/Z_d Z_{d+1}$として$x_d$，$x_{d+1}$を求める。その後ステップ４３１３へ行く。ステップ４３１３として、$x_d$，$x_{d+1}$を出力する。上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1=1$ととることにより３Ｍ＋２Ｓとなる。ここでＭは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ４３０７において加算の計算量、ステップ４３０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ４３１０において加算の計算量、ステップ４３１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ４３０４、ステップ４３０５、ステップ４３０６、ステップ４３０７、

ステップ４３０８、ステップ４３０９乃至はステップ４３０４、ステップ４３０５、ステップ４３０６、ステップ４３１０、ステップ４３１１、ステップ４３１２の繰り返しの回数は、（スカラー値dのビット長）—１回となるので、ステップ４３０２での２倍算の計算量及びアフィン座標への変換の計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋２Ｍ—２Ｓ＋Ｉとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度、計算量ＩはＩ＝４０Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋４０．４）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１５１２Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT' 98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６４０Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びモンゴメリ型楕円曲線上の点Pから、$x_d$、$x_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は5Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋４０．４）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍ及びＩ＝４０Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋８６．

2）Mと見積もることができる。例えばスカラー値dが１６０ビット（k＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１５５８Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Mであり、これと比べて必要となる計算量は削減されている。

第１７の実施例は、楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部１０３の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部１０３の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力するものである。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、x及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図３７により、座標x、y、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$が与えられた場合に$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、ワイエルシュトラス型楕円曲線において射影座標で表

されたスカラー倍点dP＝($X_d$, $Y_d$, $Z_d$)の座標うち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点($x_d$, $y_d$)を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を(X1, Y1, Z1)でそれぞれ表す。入力されたスカラー値をdとしてワイエルシュトラス型楕円曲線におけるスカラー倍点dPのアフィン座標を($x_d$, $y_d$)で、射影座標を($X_d$, $Y_d$, $Z_d$)でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点(d+1)Pのアフィン座標を($x_{d+1}$, $y_{d+1}$)で、射影座標を($X_{d+1}$, $Y_{d+1}$, $Z_{d+1}$)でそれぞれ表す。

ステップ３７０１において$x \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ３７０２において$X_d+T_1$が計算される。ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d+X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３７０３において$X_d-T_1$が計算され、ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d-X_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３７０４においてレジスタ$T_3$の２乗が計算される。ここでレジスタ$T_3$には$xZ_d-X_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３７０５において$T_3 \times X_{d+1}$が計算される。ここでレジスタ$T_3$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３７０６において$x \times X_d$が計算され、レジスタ$T_1$に格納される。ステップ３７０７において$a \times Z_d$が計算され、レジスタ$T_4$に格納される。ステップ３７０８において$T_1+T_4$が計算される。ここでレジスタ$T_1$には$xX_d$がレジスタ$T_4$には$aZ_d$がそれぞれ格納されており、したがって$xX_d+aZ_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３７０９において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$xX_d+aZ_d$がレジスタ$T_2$には$xZ_d+X_d$がそれぞれ格納されており、したがって$(xX_d+aZ_d)(xZ_d+X_d)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３７１０におい

てレジスタ$Z_d$の２乗が計算され、レジスタ$T_2$に格納される。ステップ３７１１において$T_2 \times 2b$が計算される。ここでレジスタ$T_2$には$Z_d^2$が格納されており、したがって$2bZ_d^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３７１２において$T_1+T_2$が計算される。ここでレジスタ$T_1$には$(xX_d+aZ_d)(xZ_d+X_d)$がレジスタ$T_2$には$2bZ_d^2$がそれぞれ格納されており、したがって$(xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３７１３において$T_1 \times Z_{d+1}$が計算される。ここでレジスタ$T_1$には$(xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2$が格納されており、したがって$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３７１４において$T_1-T_3$が計算される。ここでレジスタ$T_1$には$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2)$がレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2)-X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３７１５において$2y \times Z_d$が計算され、レジスタ$T_2$に格納される。ステップ３７１６において$T_2 \times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$2yZ_d$が格納されており、したがって$2yZ_dZ_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３７１７において$T_2 \times Z_d$が計算される。ここでレジスタ$T_2$には$2yZ_dZ_{d+1}$が格納されており、したがって$2yZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３７１８においてレジスタ$T_3$の逆元が計算される。ここでレジスタ$T_3$には$2yZ_dZ_{d+1}Z_d$が格納されており、したがって$1/2yZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３７１９において$T_1 \times T_3$が計算される。ここでレジスタ$T_1$には$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2)-X_{d+1}(X_d-xZ_d)^2$がレジスタ$T_3$には$1/2yZ_dZ_{d+1}Z_d$がそれぞれ格納されており、したがって$(Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2)-X_{d+1}(X_d-xZ_d)^2)/2yZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$y_d$に格納される。ステップ３７２０において$T_2 \times X_d$が計算される。ここでレジスタ$T_2$には$2yZ_dZ_{d+1}$が格納されており、したがって$2yZ_dZ_{d+1}X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３７２１において$T_2 \times T_3$が計算される。ここでレジ

スタ$T_2$には$2yZ_dZ_{d+1}X_d$がレジスタ$T_3$には$1/2yZ_dZ_{d+1}Z_d$がそれぞれ格納されており、したがって$2yZ_dZ_{d+1}X_d/2yZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$x_d$に格納される。したがってレジスタ$x_d$には$2yZ_dZ_{d+1}X_d/2yZ_dZ_{d+1}Z_d$が格納されている。レジスタ$y_d$にはステップ３７１９において$(Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2)/2yZ_dZ_{d+1}Z_d$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により、与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点のアフィン座標$(x_d, y_d)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数２７を得る。点P及び点dPはワイエルシュトラス型楕円曲線上の点であるので、$y_d{}^2=x_d{}^3+ax_d+b$及び$y^2=x^3+ax+b$をみたす。数２７に代入し、$y_d{}^2$及び$y^2$を消去し、式を整理すると、

$$y_d=\{(x_dx+a)(x_d+x)+2b-(x_d-x)^2x_{d+1}\}/(2y) \quad \cdots 数７０$$

を得る。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d=\{Z_{d+1}((X_dx+aZ_d)(X_d+xZ_d)-2bZ_d^2)-(X_d-xZ_d)^2X_{d+1}\}/(2yZ_dZ_{d+1}Z_d) \quad \cdots 数７１$$

$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、

$$x_d=(2yZ_dZ_{d+1}X_d)/(2yZ_dZ_{d+1}Z_d) \quad \cdots 数７２$$

となる。ここで、$x_d$，$y_d$は図３７で示した処理により与えられる。したがって、アフィン座標$(x_d, y_d)$の値が全て復元されていることになる。

上記手順はステップ３７０１、ステップ３７０５、ステップ３７０６、ステップ３７０７、ステップ３７０９、ステップ３７１０、ステップ３７１１、ステップ３７１３、ステップ３７１５、ステップ３７１６、ステップ３７１７、ステップ３７１９、ステップ３７２０及びステップ３７２１において有限体上の乗算の計算量を必要とする。また、ステップ３７０４において有限体上の２乗算の計算量を必要とする。また、ステップ３７１８において有限体上の逆元演算の計算量

を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１４Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００Ｍ弱と見積もられる。Ｓ＝０．８Ｍ、Ｉ＝４０Ｍと仮定すると座標復元の計算量は５４．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$，$y_d$の値が計算できれば$x_d$，$y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。

次に図４４により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d, Z_d, X_{d+1}, Z_{d+1}$を出力する高速スカラー倍計算部の処理について説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$のうち$X_{d+1}$及び$Z_{d+1}$を出力する。ステップ４４１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ４４０１として、変数Ｉに初期値１を代入する。ステップ４４０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において$(x, y, 1)$として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ４４０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ４４０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ４４０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すれ

ばステップ４４１５へ行く。一致しなければステップ４４０５へ行く。ステップ４４０５として、変数Ｉを１増加させる。ステップ４４０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ４４０７へ行く。そのビットの値が１であればステップ４４１０へ行く。ステップ４４０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ４４０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４４０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ４４０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４４０９として、ステップ４４０８で求めた点2mPとステップ４４０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ４４０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ４４１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ４４１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４４１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ４４１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４４１２として、ステップ４４１０で求めた点(2m+１)Pとステップ４４１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ４４０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ４４１５として、モンゴメリ型楕円曲線における点(m−1)Pを、ワイエルシュトラス型楕円曲線上で射影座標により表された点に変換する。その点のX座標及びZ座標をそれぞれあらためてXm−1及びZm−1とおく。また、モンゴメリ型楕円曲線において射影座標

で表された点の組(mP, (m+1)P)に対して、点mP及び点(m+1)Pをワイエルシュトラス型楕円曲線上で射影座標で表された点に変換し、それぞれmP＝（$X_m$, $Y_m$, $Z_m$）及び(m+1)P＝（$X_{m+1}$, $Y_{m+1}$, $Z_{m+1}$）とあらためて置き直す。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。ステップ４４１３として、ワイエルシュトラス型楕円曲線上で射影座標で表された点mP＝（$X_m$, $Y_m$, $Z_m$）より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$として、ワイエルシュトラス型楕円曲線上で射影座標で表された点(m+1)P＝（$X_{m+1}$, $Y_{m+1}$, $Z_{m+1}$）より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$として、出力する。また上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等しくなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、Z1=1ととることにより３Ｍ＋２Ｓとなる。ここでMは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ４４０７において加算の計算量、ステップ４４０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ４４１０において加算の計算量、ステップ４４１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ４４０４、ステップ４４０５、ステップ４４０６、ステップ４４０７、ステップ４４０８、ステップ４４０９乃至はステップ４４０４、ステップ４４０５、ステップ４４０６、ステップ４４１０、ステップ４４１１、ステップ４４１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ４４０２での２倍算の計算量とステップ４４１６でのモンゴメリ型楕円曲線上の点への変換に必要な計算量及びステップ４４１５でのワイエルシュトラス型楕円曲線上の点への変換に必要な計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋２Ｍ－２Ｓとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度と見積もられるので、全体の計算量は

おおよそ（９．２ｋ＋０．４）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１４７２Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT' 98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６００Ｍとなる。したがって、上記本発明による手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１４Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋０．４）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５５．２）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１５２７Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第１８の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたもの

である。すなわち、スカラー倍計算部１０３の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部１０３の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、x及びyよりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標$X_d, Y_d$及び$Z_d$の復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を計算結果として出力する。

次に図３８により、座標x、y $X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$が与えられた場合に$X_d$、$Y_d$、$Z_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、ワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたワイエルシュトラス型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pをアフィン座標で表した$(x, y)$を入力し、以下の手順で射影座標おいて完全な座標が与えられたスカラー倍点$(X_d, Y_d, Z_d)$を出力する。ここで入力されたワイエルシュトラス型楕円曲線上の点Pのアフィン座標を$(x, y)$で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとして

ワイエルシュトラス型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。ワイエルシュトラス型楕円曲線上の点$(_{d+1})$Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ３８０１において$x \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ３８０２において$X_d+T_1$が計算される。ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d+X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３８０３において$X_d-T_1$が計算され、ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d-X_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３８０４においてレジスタ$T_3$の２乗が計算される。ここでレジスタ$T_3$には$xZ_d-X_d$ が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３８０５において$T_3 \times X_{d+1}$が計算される。ここでレジスタ$T_3$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ３８０６において$x \times X_d$が計算され、レジスタ$T_1$に格納される。ステップ３８０７において$a \times Z_d$が計算され、レジスタ$T_4$に格納される。ステップ３８０８において$T_1+T_4$が計算される。ここでレジスタ$T_1$には$xX_d$がレジスタ$T_4$には$aZ_d$がそれぞれ格納されており、したがって$xX_d+aZ_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３８０９において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$xX_d+aZ_d$がレジスタ$T_2$には$xZ_d+X_d$がそれぞれ格納されており、したがって$(xX_d+aZ_d)(xZ_d+X_d)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３８１０においてレジスタ$Z_d$の２乗が計算され、レジスタ$T_2$に格納される。ステップ３８１１において$T_2 \times 2b$が計算される。ここでレジスタ$T_2$には$Z_d^2$が格納されており、したがって$2bZ_d^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３８１２において$T_1+T_2$が計算される。ここでレジスタ$T_1$には$(xX_d+aZ_d)(xZ_d+X_d)$がレジスタ$T_2$には$2bZ_d^2$がそれぞれ格納されており、したがって$(xX_d+aZ_d)(xZ_d+X_d)+2bZ_d^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３８１３において$T_1 \times Z_{d+1}$が計算される。ここでレ

ジスタ$T_1$には$(xX_d+aZ_d)(xZ_d+X_d)+2bZ_d{}^2$が格納されており、したがって$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d{}^2)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３８１４において$T_1-T_3$が計算される。ここでレジスタ$T_1$には$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d{}^2)$がレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$Y_d$に格納される。ステップ３８１５において$2y\times Z_d$が計算され、レジスタ$T_2$に格納される。ステップ３８１６において$T_2\times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$2yZ_d$が格納されており、したがって$2yZ_dZ_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３８１７において$T_2\times X_d$が計算される。ここでレジスタ$T_2$には$2yZ_dZ_{d+1}$が格納されており、したがって$2yZ_dZ_{d+1}X_d$が計算される。その結果がレジスタ$X_d$に格納される。ステップ３８１９において$T_2\times Z_d$が計算される。ここでレジスタ$T_2$には$2yZ_dZ_{d+1}$が格納されており、したがって$2yZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$Z_d$に格納される。したがってレジスタ$Z_d$には$2yZ_dZ_{d+1}Z_d$が格納されている。レジスタ$Y_d$にはステップ３８１４において$Z_{d+1}((xX_d+aZ_d)(xZ_d+X_d)+2bZ_d{}^2)+X_{d+1}(X_d-xZ_d)^2$が格納され、その後更新が行なわれないので、その値が保持されている。レジスタ$X_d$にはステップ３８１７において$2yZ_dZ_{d+1}X_d$が格納され、その後更新が行なわれないので、その値が保持されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標$(X_d,Y_d,Z_d)$における値が全て復元される理由は以下の通りである。点$(d+1)P$は点$dP$に点$P$を加算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数２７を得る。点P及び点dPはワイエルシュトラス型楕円曲線上の点であるので、$y_d{}^2=x_d{}^3+ax_d+b$及び$y^2=x^3+ax+b$をみたす。数２７に代入し、$y_d{}^2$及び$y^2$を消去し、式を整理すると、数７０を得る。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$であり、この値を代入することにより射影座標の値へと変換すると、数７１を得る。$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、数７２となる。その結果として

$Y_d = Z_{d+1}[(X_d x + aZ_d)(X_d + xZ_d) + 2bZ_d^2] - (X_d - xZ_d)^2 X_{d+1}$ …数７３

とし、$X_d$及び$Z_d$をそれぞれ

$2yZ_d Z_{d+1} X_d$ …数７４

$2yZ_d Z_{d+1} Z_d$ …数７５

により更新すればよい。ここで、$X_d$，$Y_d$，$Z_d$は図３８で示した処理により与えられる。したがって、射影座標$(X_d, Y_d, Z_d)$の値は全て復元されたことになる。

上記手順はステップ３８０１、ステップ３８０５、ステップ３８０６、ステップ３８０７、ステップ３８０９、ステップ３８１１、ステップ３８１３、ステップ３８１５、ステップ３８１６、ステップ３８１７及びステップ３８１８において有限体上の乗算の計算量を必要とする。また、ステップ３８０４およびステップ３８１０において有限体上の２乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をSとすると、上記手順は１１M＋２Sの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００M弱と見積もられる。S＝０．８Mと仮定すると座標復元の計算量は１２．６Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d, Y_d, Z_d$の値が計算できれば$X_d, Y_d, Z_d$の値が復元できる。また、$x_d, y_d$が上記計算式により与えられる値を取るように$X_d, Y_d, Z_d$の値を選択し、その値が計算できれば$X_d$, $Y_d, Z_d$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムについて説明する。

第１８実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第１７実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力

するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１１M＋２Sであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２k＋０．４）Mとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。S＝０．８Mと仮定すると、この計算量はおおよそ（９．２k＋１３）Mと見積もることができる。例えばスカラー値dが１６０ビット（k＝１６０）であれば、このスカラー倍計算に必要な計算量はおおよそ１４８５Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Mであり、これと比べて必要となる計算量は削減されている。

第１９の実施例は楕円曲線としてワイエルシュトラス型楕円曲線を用いたものである。すなわち、スカラー倍計算部１０３の入出力に用いる楕円曲線はワイエルシュトラス型楕円曲線である。ただし、スカラー倍計算部１０３の内部の計算で使用する楕円曲線として、与えられたワイエルシュトラス型楕円曲線から変換可能であるようなモンゴメリ型楕円曲線を用いてもよい。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d, y_d)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標の

うち$x_d$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝($x_{d+1}$, $y_{d+1}$)の座標のうち$x_{d+1}$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点($_d$-1)P＝($x_d$-1, $y_d$-1)の座標のうち$x_d$-1を計算し、アフィン座標で表された入力されたワイエルシュトラス型楕円曲線上の点P＝(x, y)と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$x_d$、$x_{d+1}$、$x_{d-1}$、x及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝($x_d$, $y_d$)の座標$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点($x_d$, $y_d$)を計算結果として出力する。

次に図３９により、座標x、y、$x_d$、$x_{d+1}$が与えられた場合に、$x_d$、$y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、ワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝($x_d$, $y_d$)の座標のうち$x_d$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝($x_{d+1}$, $y_{d+1}$)の座標のうち$x_{d+1}$、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点($x_d$, $y_d$)を出力する。

ステップ３９０１において$x_d$×xが計算され、レジスタ$T_1$に格納される。ステップ３９０２において$T_1$+aが計算される。ここでレジスタ$T_1$には$x_d$xが格納されており、したがって$x_d$x+aが計算される。その結果がレジスタ$T_1$に格納される。ステップ３９０３において$x_d$+xが計算され、レジスタ$T_2$に格納される。ステップ３９０４において$T_1$×$T_2$が計算される。ここでレジスタ$T_1$には$x_d$x+aがレジスタ$T_2$には$x_d$+xがそれぞれ格納されており、したがって($x_d$x+a)($x_d$+x)が計算される。その結果がレジスタ$T_1$に格納される。ステップ３９０５において$T_1$+2bが計算される。ここでレジスタ$T_1$には($x_d$x+a)($x_d$+x)が格納されており、したがって($x_d$x+a)($x_d$+x)+2bが計算される。その結果がレジスタ$T_1$に格納される。ステップ３９０６において$x_d$-xが計算され、レジスタ$T_2$に格納される。ステップ３９０７において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$x_d$-xが格納されており、したがって$(x_d-x)^2$が計算さ

れる。その結果がレジスタ$T_2$に格納される。ステップ３９０８において$T_2$×$x2_{d+1}$が計算される。ここでレジスタ$T_2$には$(x_d-x)^2$が格納されており、したがって$x_{d+1}(x_d-x)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ３９０９において$T_1$-$T_2$が計算される。ここでレジスタ$T_1$には$(x_dx+a)(x_d+x)+2b$がレジスタ$T_2$には$x_{d+1}(x_d-x)^2$がそれぞれ格納されており、したがって$(x_dx+a)(x_d+x)+2b-x_{d+1}(x_d-x)^2$が計算される。その結果がレジスタ$T_1$に格納される。ステップ３９１０において2yの逆元が計算され、レジスタ$T_2$に格納される。ステップ３９１１において$T_1$×$T_2$が計算される。ここでレジスタ$T_1$には$(x_dx+a)(x_d+x)+2b-x_{d+1}(x_d-x)^2$がレジスタ$T_2$には1/2yがそれぞれ格納されており、したがって$((x_dx+a)(x_d+x)+2b-x_{d+1}(x_d-x)^2)/2y$が計算される。その結果がレジスタ$y_d$に格納される。したがってレジスタ$y_d$には$((x_dx+a)(x_d+x)+2b-x_{d+1}(x_d-x)^2)/2y$が格納されている。レジスタ$x_d$は全く更新されないので入力された値が保持されている。

上記手順によりスカラー倍点のy座標$y_d$が復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。ワイエルシュトラス型楕円曲線のアフィン座標における加算公式に代入すると、数２７を得る。点P及び点dPはワイエルシュトラス型楕円曲線上の点であるので、$y_d^2=x_d^3+ax_d+b$及び$y^2=x^3+ax+b$をみたす。数２７に代入し、$y_d^2$及び$y^2$を消去し、式を整理すると、数７０を得る。ここで$x_d$, $y_d$は図３９の処理によって与えられる。したがって、アフィン座標$(x_d, y_d)$の値を全て復元していることになる。

上記手順はステップ３９０１、ステップ３９０４、ステップ３９０８及びステップ３９１１において有限体上の乗算の計算量を必要とする。また、ステップ３９０７において有限体上の２乗算の計算量を必要とする。さらにステップ３９１０において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をＳ、有限体上の逆元演算の計算量をＩとすると、上記手順は４Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー

倍計算の計算量はおおよそ１５００M弱と見積もられる。Ｓ＝０．８M及びＩ＝４０Mと仮定すると座標復元の計算量は４４．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば$y_d$の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。

次に図４４により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$、$x_{d+1}$を出力するアルゴリズムについて説明する。

高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$のうち$x_d$、アフィン座標で表されたワイエルシュトラス型楕円曲線上の点(d+1)P＝$(x_{d+1}, y_{d+1})$のうち$x_{d+1}$を出力する。ステップ４４１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ４４０１として、変数Ｉに初期値１を代入する。ステップ４４０２として、点Pの２倍点２Pを計算する。ここで点Pは射影座標において(ｘ，ｙ，1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ４４０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ４４０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ４４０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ４４１５へ行く。一致しなければステップ４４０５へ行く。ステップ４４０５として、変数Ｉを１増加させる。ステップ４４０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ４４０６へ行く。そのビットの値が１であればステップ４４１０へ行く。ステップ４４０７として、射影座標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ４４０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標におけ

る加算公式を用いて計算される。ステップ４４０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算２(mP)を行ない、点2mPを計算する。その後ステップ４４０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４４０９として、ステップ４４０８で求めた点2mPとステップ４４０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ４４０４へ戻る。ここで、点２mP、点(２m+１)P、点mP及び点(m+１)Pは全て射影座標において表されている。ステップ４４１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+１)Pの加算mP+(m+１)Pを行ない、点(2m+１)Pを計算する。その後ステップ４４１１へ行く。ここで、加算mP+(m+１)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４４１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ４４１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４４１２として、ステップ４４１０で求めた点(2m+１)Pとステップ４４１１で求めた点(2m+2)Pを点の組((2m+1)P, (2m+2)P)として、点の組(mP, (m+1)P)の代わりに格納する。その後ステップ４４０４へ戻る。ここで、点(2m+1)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ４４１５として、モンゴメリ型楕円曲線において射影座標で表された点の組(mP, (m+1)P)に対して、点mP及び点(m+1)Pをワイエルシュトラス型楕円曲線上でアフィン座標で表された点に変換し、それぞれmP＝ $(x_m, y_m)$ 及び(m+1)P＝ $(x_{m+1}, y_{m+1})$ とあらためて置き直す。ここで、$y_m$及び$y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。その後ステップ４４１３へ行く。ステップ４４１３として、ワイエルシュトラス型楕円曲線上で射影座標で表された点mP＝ $(x_m, y_m)$ より$x_m$を$x_d$として、ワイエルシュトラス型楕円曲線上でアフィン座標で表された点(m+1)P＝ $(x_{m+1}, y_{m+1})$ より$x_{m+1}$を$x_{d+1}$として、出力する。また上記手順により、ｍとスカラー値dはビット長が等しくさらにそのビットのパターンも同じとなる為、等し

くなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1$＝１ととることにより３Ｍ＋２Ｓとなる。ここでＭは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ４４０７において加算の計算量、ステップ４４０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ４４１０において加算の計算量、ステップ４４１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ４４０４、ステップ４４０５、ステップ４４０６、ステップ４４０７、ステップ４４０８、ステップ４４０９乃至はステップ４４０４、ステップ４４０５、ステップ４４０６、ステップ４４１０、ステップ４４１１、ステップ４４１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ４４０２での２倍算の計算量とステップ４４１６でのモンゴメリ型楕円曲線上への点への変換に必要な計算量及びステップ４４１５でのワイエルシュトラス型楕円曲線上の点への必要な計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋４Ｍ－２Ｓ＋Ｉとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度、計算量Ｉは、Ｉ＝４０Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋４２．４）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１５１４Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられる。例えばスカラー値dが１６０ビット（ｋ

＝１６０）であれば、このスカラー倍計算方法の計算量はおおよそ１６４０Mとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$, $x_{d+1}$, $x_{d-1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は４M＋S＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２k＋４２．４）Mとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０M、S＝０．８Mと仮定すると、この計算量はおおよそ（９．２k＋８７．２）Mと見積もることができる。例えばスカラー値dが１６０ビット（k＝１６０）であれば、このスカラー倍計算に必要な計算量は１５５９Mとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Mであり、これと比べて必要となる計算量は削減されている。

第２０の実施例は、入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Ｐから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点（$x_d$, $y_d$）を計算し出力するものである。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Ｐからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝($X_d$, $Y_d$, $Z_d$)の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d＋1)P＝

$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たにP＝(x, y)とおく。高速スカラー倍計算部２０２は、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、ｘ及びｙを座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$、ｘ及びｙよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点dP＝$(x_d, y_d)$の座標$x_d$及び$y_d$の復元を行なう。スカラー倍計算部１０３はアフィン座標において完全に座標が与えられたスカラー倍点$(x_d, y_d)$を計算結果として出力する。

次に図４０により、座標$x, y, X_d, Z_d, X_{d+1}, Z_{d+1}$が与えられた場合に$x_d, y_d$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点dP＝$(X_d, Y_d, Z_d)$の座標うち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点(d+1)P＝$(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でアフィン座標おいて完全な座標が与えられたスカラー倍点$(x_d, y_d)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を(X１, Y１, Z１)でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d^{Mon}, y_d^{Mon})$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ４００１において$x \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ４００２において$X_d + T_1$が計算される。ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d + X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４００３において$X_d - T_1$が計算され、ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d - X_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４００４においてレジスタ$T_3$の２乗が計算される。ここでレジスタ$T_3$には$xZ_d - X_d$が格納されており、したがって$(X_d -$

$xZ_d)^2$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ４００５においてＴ$_3 \times X_{d+1}$が計算される。ここでレジスタＴ$_3$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)2$が計算される。その結果がレジスタＴ$_3$に格納される。ステップ４００６において$2A \times Z_d$が計算され、レジスタＴ$_1$に格納される。ステップ４００７においてＴ$_2$+Ｔ$_1$が計算される。ここでレジスタＴ$_2$には$xZ_d+X_d$がレジスタＴ$_1$には$2AZ_d$がそれぞれ格納されており、したがって$xZ_d+X_d+2AZ_d$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ４００８において$x \times X_d$が計算され、レジスタＴ$_4$に格納される。ステップ４００９においてＴ$_4+Z_d$が計算される。ここでレジスタＴ$_4$には$xX_d$が格納されており、したがって$xX_d+Z_d$が計算される。その結果がレジスタＴ$_4$に格納される。ステップ４０１０においてＴ$_2 \times$Ｔ$_4$が計算される。ここでレジスタＴ$_2$には$xZ_d+X_d+2AZ_d$がレジスタＴ$_4$には$xX_d+Z_d$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ４０１１においてＴ$_1 \times Z_d$が計算される。ここでレジスタＴ$_1$には$2AZ_d$が格納されており、したがって$2AZ_d{}^2$が計算される。その結果がレジスタＴ$_1$に格納される。ステップ４０１２においてＴ$_2$−Ｔ$_1$が計算される。ここでレジスタＴ$_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$がここでレジスタＴ$_1$には$2AZ_d{}^2$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ４０１３においてＴ$_2 \times Z_{d+1}$が計算される。ここでレジスタＴ$_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2$が格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ４０１４においてＴ$_2$−Ｔ$_3$が計算される。ここでレジスタＴ$_2$には$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)$がレジスタＴ$_3$には$X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタＴ$_2$に格納される。ステップ４０１５において$2B \times y$が計算され、レジスタＴ$_1$に格納される。ステップ４０１６においてＴ$_1 \times Z_d$が計算される。ここでレジスタＴ$_1$には$2By$が格納されており、したがって$2ByZ_d$が計算される。その結果がレジスタ

$T_1$に格納される。ステップ４０１７において$T_1 \times Z_{d+1}$が計算される。ここでレジスタ$T_1$には$2ByZ_d$が格納されており、したがって$2ByZ_dZ_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４０１８において$T_1 \times Z_d$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}$が格納されており、したがって$2ByZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４０１９において$T_3 \times s$が計算される。ここでレジスタ$T_3$には$2ByZ_dZ_{d+1}Z_d$が格納されており、したがって$2ByZ_dZ_{d+1}Z_ds$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４０２０においてレジスタ$T_3$の逆元が計算される。ここでレジスタ$T_3$には$2ByZ_dZ_{d+1}Z_ds$が格納されており、したがって$1/2ByZ_dZ_{d+1}Z_ds$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４０２１において$T_2 \times T_3$が計算される。ここでレジスタ$T_2$には$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2$がレジスタ$T_3$には$1/2ByZ_dZ_{d+1}Z_ds$がそれぞれ格納されており、したがって$\{Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2\}/2ByZ_dZ_{d+1}Z_ds$が計算される。その結果がレジスタ$y_d$に格納される。ステップ４０２２において$T_1 \times X_d$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}$が格納されており、したがって$2ByZ_dZ_{d+1}X_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４０２３において$T_1 \times T_3$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}X_d$がレジスタ$T_3$には$1/2ByZ_dZ_{d+1}Z_ds$がそれぞれ格納されており、したがって$2ByZ_dZ_{d+1}X_d/2ByZ_dZ_{d+1}Z_ds(=X_d/Z_ds)$が計算される。その結果が$T_1$に格納される。ステップ４０２４において$T_1+\alpha$が計算される。ここでレジスタ$T_1$には$X_d/Z_ds$が格納されており、したがって$(X_d/Z_ds)+\alpha$が計算される。その結果が$x_d$に格納される。したがってレジスタ$x_d$には$(X_d/Z_ds)+\alpha$の値が格納されている。$y_d$にはステップ４０２１において$\{Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d{}^2)-X_{d+1}(X_d-xZ_d)^2\}/2ByZ_dZ_{d+1}Z_ds$が格納され、その後更新が行なわれないので、その値が保持されている。その結果として、ワイエルシュトラス型楕円曲線におけるアフィン座標$(x_d, y_d)$の値が全て復元されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からワイエルシ

ュトラス型楕円曲線におけるスカラー倍点のアフィン座標( $x_d$ , $y_d$ )における値が全て復元される理由は以下の通りである。点(d+1)Pは点 $_d$ Pに点Pを加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数３８を得る。点P及び点dPはモンゴメリ型楕円曲線上の点であるので、 $By_d^{Mon\,2}=x_d^{Mon\,3}+Ax_d^{Mon\,2}+x_d^{Mon}$ 及び $By^2=x^3+Ax^2+x$ をみたす。数３８に代入し、 $By_d^{Mon\,2}$ 及び $By^2$ を消去し、式を整理すると、

$$y_d^{Mon}=\{(x_d^{Mon}x+1)(x_d^{Mon}+x+2A)-2A-(x_d^{Mon}-x)^2x_{d+1}\}/(2By) \quad \cdots数７６$$

を得る。ここで $x_d^{Mon}=X_d/Z_d$ 、 $x_{d+1}=X_{d+1}/Z_{d+1}$ であり、この値を代入することにより射影座標の値へと変換すると、次の式を得る。

$$y_d^{Mon}=\{Z_{d+1}\left((X_dx+Z_d)(X_d+xZ_d+2AZ_d)-2AZ_d^2\right)-(x_d-xZ_d)^2X_{d+1}\}/(2ByZ_dZ_{d+1}Z_d) \quad \cdots数７７$$

$x_d^{Mon}=X_d/Z_d$ であるが、逆元演算の回数を減らす目的で $y_d^{Mon}$ の分母と通分することにより、

$$x_d^{Mon}=(2ByZ_dZ_{d+1}X_d)/(2ByZ_dZ_{d+1}Z_d) \quad \cdots数７８$$

となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form an $_d$ Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをs, αとして、 $y_d=s^{-1}y_d^{Mon}$ 及び $x_d=s^{-1}x_d^{Mon}+\alpha$ の関係がある。結果として数７９、数８０を得る。

$$y_d=\{Z_{d+1}\left((X_dx+Z_d)(X_d+xZ_d+2AZ_d)-2AZ_d^2\right)-(X_d-xZ_d)^2X_{d+1}\}/(2sByZ_dZ_{d+1}Z_d) \quad \cdots数７９$$

$$x_d=((2ByZ_dZ_{d+1}X_d)/(2sByZ_dZ_{d+1}Z_d))+\alpha \quad \cdots数８０$$

ここで、 $x_d$ , $y_d$ は図４０より与えられる。したがって、ワイエルシュトラス型楕円曲線におけるアフィン座標( $x_d$ , $y_d$ )の値が全て復元されていることになる。

上記手順はステップ４００１、ステップ４００５、ステップ４００６、ステップ４００８、ステップ４０１０、ステップ４０１１、ステップ４０１３、ステップ４０１５、ステップ４０１６、ステップ４０１７、ステップ４０１８、ステッ

プ４０１９、ステップ４０２１、ステップ４０２２及びステップ４０２３において有限体上の乗算の計算量を必要とする。また、ステップ４００４において有限体上の２乗算の計算量を必要とする。また、ステップ４０２０において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量及び逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳ及び有限体上の逆元演算の計算量をＩとすると、上記手順は１５Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００Ｍ弱と見積もられる。Ｓ＝０．８Ｍ、Ｉ＝４０Ｍと仮定すると座標復元の計算量は５５．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$x_d$，$y_d$の値が計算できれば$x_d$，$y_d$の値が復元できる。その場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタであるA乃至はBの値やモンゴメリ型楕円曲線への変換パラメタであるｓを小さくとることにより、ステップ４００６乃至はステップ４０１５における乗算の計算量やステップ４０１９における乗算の計算量を削減することができる。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力する高速スカラー倍計算部の処理について説明する。

この場合、第２０実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第９実施例の高速スカラー倍計算方法（図８参照）を用いる。これにより、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記アルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量

は１５Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ－３．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋５２．２）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１５２４Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

第２１の実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３がスカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線における射影座標の点として完全な座標が与えられたスカラー倍点, $(X_d{}^W, Y_d{}^W, Z_d{}^W)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$_dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$_{(d+1)}P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$を計算する。また、入力されたワイエルシュトラス型楕円曲線上の点Pを、与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線上の点に変換し、その点を新たにP=(x, y)とおく。高速スカラー倍計算部２０２は、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，x及びyを座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$，x及びyよりワイエルシュトラス型楕円曲線において射影座標で表されたスカラー倍点dP=$(X_d{}^W, Y_d{}^W, Z_d{}^W)$の座標$X_d{}^W$、$Y_d{}^W$及び$Z_d{}^W$の

復元を行なう。スカラー倍計算部１０３は射影座標において完全に座標が与えられたスカラー倍点$(X_d{}^W, Y_d{}^W, Z_d{}^W)$を計算結果として出力する。

次に図４１により、座標x, y, $X_d$, $Z_d$, $X_{d+1}$, $Z_{d+1}$が与えられた場合に$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線において射影座標で表されたスカラー倍点$dP=(X_d, Y_d, Z_d)$の座標のうち$X_d$及び$Z_d$、射影座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(X_{d+1}, Y_{d+1}, Z_{d+1})$の座標のうち$X_{d+1}$及び$Z_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した(x, y)を入力し、以下の手順でワイエルシュトラス型楕円曲線上で射影座標おいて完全な座標が与えられたスカラー倍点$(X_d{}^W, Y_d{}^W, Z_d{}^W)$を出力する。ここで入力されたモンゴメリ型楕円曲線上の点Pのアフィン座標を(x, y)で、射影座標を$(X_1, Y_1, Z_1)$でそれぞれ表す。入力されたスカラー値をdとしてモンゴメリ型楕円曲線におけるスカラー倍点dPのアフィン座標を$(x_d, y_d)$で、射影座標を$(X_d, Y_d, Z_d)$でそれぞれ表す。モンゴメリ型楕円曲線上の点(d+1)Pのアフィン座標を$(x_{d+1}, y_{d+1})$で、射影座標を$(X_{d+1}, Y_{d+1}, Z_{d+1})$でそれぞれ表す。

ステップ４１０１において$x \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ４１０２において$X_d+T_1$が計算される。ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d+X_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４１０３において$X_d-T_1$が計算され、ここでレジスタ$T_1$には$xZ_d$が格納されており、したがって$xZ_d-X_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４１０４においてレジスタ$T_3$の２乗が計算される。ここでレジスタ$T_3$には$xZ_d-X_d$が格納されており、したがって$(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４１０５において$T_3 \times X_{d+1}$が計算される。ここでレジスタ$T_3$には$(X_d-xZ_d)^2$が格納されており、したがって$X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４１０６において$2A \times Z_d$が計算され、レジスタ$T_1$に格納される。ステップ４１０７において$T_2+T_1$が計算される。ここでレジスタ$T_2$には$xZ_d+X_d$がレジスタ$T_1$には$2AZ_d$がそれぞれ格納されており、した

がって$xZ_d+X_d+2AZ_d$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４１０８において$x\times X_d$が計算され、レジスタ$T_4$に格納される。ステップ４１０９において$T_4+Z_d$が計算される。ここでレジスタ$T_4$には$xX_d$が格納されており、したがって$xX_d+Z_d$が計算される。その結果がレジスタ$T_4$に格納される。ステップ４１１０において$T_2\times T_4$が計算される。ここでレジスタ$T_2$には$xZ_d+X_d+2AZ_d$がレジスタ$T_4$には$xX_d+Z_d$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４１１１において$T_1\times Z_d$が計算される。ここでレジスタ$T_1$には$2AZ_d$が格納されており、したがって$2AZ_d^{\,2}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４１１２において$T_2-T_1$が計算される。ここでレジスタ$T_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)$がここでレジスタ$T_1$には$2AZ_d^{\,2}$がそれぞれ格納されており、したがって$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^{\,2}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４１１３において$T_2\times Z_{d+1}$が計算される。ここでレジスタ$T_2$には$(xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^{\,2}$が格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^{\,2})$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４１１４において$T_2-T_3$が計算される。ここでレジスタ$T_2$には$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^{\,2})$がレジスタ$T_3$には$X_{d+1}(X_d-xZ_d)^2$がそれぞれ格納されており、したがって$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^{\,2})-X_{d+1}(X_d-xZ_d)^2$が計算される。その結果がレジスタ$Y_d^{\,W}$に格納される。ステップ４１１５において$2B\times y$が計算され、レジスタ$T_1$に格納される。ステップ４１１６において$T_1\times Z_d$が計算される。ここでレジスタ$T_1$には$2By$が格納されており、したがって$2ByZ_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４１１７において$T_1\times Z_{d+1}$が計算される。ここでレジスタ$T_1$には$2ByZ_d$が格納されており、したがって$2ByZ_dZ_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４１１８において$T_1\times Z_d$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}$が格納されており、したがって$2ByZ_dZ_{d+1}Z_d$が計算される。その結果がレジスタ$T_3$に格納される。ステップ４１１９において$T_3\times s$が計算される。ここでレジスタ$T_3$には

$2ByZ_dZ_{d+1}Z_d$が格納されており、したがって$2ByZ_dZ_{d+1}Z_ds$が計算される。その結果がレジスタ$Z_d^W$に格納される。ステップ４１２０において$T_1 \times X_d$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}$が格納されており、したがって$2ByZ_dZ_{d+1}X_d$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４１２１において$Z_d^W \times \alpha$が計算される。ここでレジスタ$Z_d^W$には$2ByZ_dZ_{d+1}Z_ds$が格納されており、したがって$2ByZ_dZ_{d+1}Z_ds\alpha$が計算される。その結果が$T_3$に格納される。ステップ４１２２において$T_1+T_3$が計算される。ここでレジスタ$T_1$には$2ByZ_dZ_{d+1}X_d$がレジスタ$T_3$には$2ByZ_dZ_{d+1}Z_ds\alpha$がそれぞれ格納されており、したがって$2ByZ_dZ_{d+1}X_d+2ByZ_dZ_{d+1}Z_ds\alpha$が計算される。その結果が$X_d^W$に格納される。したがってレジスタ$x_d$には$2ByZ_dZ_{d+1}X_d+2ByZ_dZ_{d+1}Z_ds\alpha$の値が格納されている。$Y_d^W$にはステップ４１１４において$Z_{d+1}((xZ_d+X_d+2AZ_d)(xX_d+Z_d)-2AZ_d^2)-X_{d+1}(X_d-xZ_d)^2$が格納され、その後更新が行なわれないので、その値が保持されている。$Z_d^W$にはステップ４１１９において$2ByZ_dZ_{d+1}Z_ds$が格納され、その後更新が行なわれないので、その値が保持されている。その結果として、ワイエルシュトラス型楕円曲線における射影座標$(X_d^W, Y_d^W, Z_d^W)$の値が全て復元されている。

上記手順により与えられた$x$、$y$、$X_d$、$Z_d$、$X_{d+1}$、$Z_{d+1}$からワイエルシュトラス型楕円曲線におけるスカラー倍点の射影座標$(X_d^W, Y_d^W, Z_d^W)$における値が全て復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６を得る。点P及び点dPはモンゴメリ型楕円曲線上の点であるので、$By_d^2=x_d^3+Ax_d^2+x_d$及び$By^2=x^3+Ax^2+x$をみたす。数６に代入し、$By_d^2$及び$By^2$を消去し、式を整理すると、数６４をを得る。ここで$x_d=X_d/Z_d$、$x_{d+1}=X_{d+1}/Z_{d+1}$であり、この値を代入することにより射影座標の値へと変換すると、数６５を得る。$x_d=X_d/Z_d$であるが、逆元演算の回数を減らす目的で$y_d$の分母と通分することにより、数６６となる。その結果として、

$$Y'_d=Z_{d+1}[(X_d+xZ_d+2AZ_d)(X_dx+Z_d)-2AZ_d^2]-(X_d-xZ_d)^2X_{d+1} \quad \cdots数８１$$

とし、

$$X'_d=2ByZ_dZ_{d+1}X_d \quad \cdots数８２$$

$$Z'_d=2ByZ_dZ_{d+1}Z_d \quad \cdots 数８３$$

とすると$(X'_d, Y'_d, Z'_d)=(X_d, Y_d, Z_d)$となる。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをsαとして、$Y_d^W=Y'_d$、$X_d^W=X'_d+\alpha Z_d^W$、及び$Z_d^W=sZ'_d$という関係がある。結果として次の式を得る。

$$Y_d^W=Z_{d+1}[(X_d+xZ_d+2AZ_d)(X_dx+Z_d)-2AZ_d^2]-(X_d-xZ_d)^2X_{d+1} \quad \cdots 数８４$$

$$X_d^W=2ByZ_dZ_{d+1}X_d+\alpha Z_d^W \quad \cdots 数８５$$

$$Z_d^W=2sByZ_dZ_{d+1}Z_d \quad \cdots 数８６$$

により更新すればよい。ここで、$X_d^W, Y_d^W, Z_d^W$は図４１の処理により与えられている。したがって、ワイエルシュトラス型楕円曲線における射影座標$(X_d^W, Y_d^W, Z_d^W)$の値が全て復元されていることになる。

上記手順はステップ４１０１、ステップ４１０５、ステップ４１０６、ステップ４１０８、ステップ４１１０、ステップ４１１１、ステップ４１１３、ステップ４１１５、ステップ４１１６、ステップ４１１７、ステップ４１１８、ステップ４１１９、ステップ４１２０及びステップ４１２１において有限体上の乗算の計算量を必要とする。また、ステップ４１０４において有限体上の２乗算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をＭ、有限体上の２乗算の計算量をＳとすると、上記手順は１４Ｍ＋Ｓの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はおおよそ１５００Ｍ弱と見積もられる。Ｓ＝０．８Ｍと仮定すると座標復元の計算量は１４．８Ｍであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記計算式により与えられた$X_d^W$、$Y_d^W$、$Z_d^W$の値が計算できれば$X_d^W$、$Y_d^W$、$Z_d^W$の値が復元できる。また、ワイエル

シュトラス型楕円曲線においてアフィン座標におけるスカラー倍点dPをdP=($x_d{}^W$, $y_d{}^W$)とすると、$x_d{}^W$、$y_d{}^W$が上記計算式により与えられる値を取るように$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$の値を選択し、その値が計算できれば$X_d{}^W$、$Y_d{}^W$、$Z_d{}^W$が復元できる。それらの場合においては一般的に復元に必要となる計算量が増大する。また、モンゴメリ型楕円曲線のパラメタであるA乃至はBの値やモンゴメリ型楕円曲線への変換パラメタsの値を小さくとることにより、ステップ４１０６、ステップ４１１５乃至はステップ４１１９における乗算の計算量を削減することができる。

次に、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムについて説明する。

第２１実施例の高速スカラー倍計算部２０２の高速スカラー倍計算方法として、第９実施例の高速スカラー倍計算方法を用いる。これにより、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムとして、高速であるアルゴリズムが達成される。尚、高速スカラー倍計算部２０２において上記アルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は１４Ｍ＋Ｓであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ－３．６）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋１１．２）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１４８３Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をヤコビアン座標として出力する場合に必要となる計算量はおおよそ１６００Ｍであり、これと比べて必要となる計算量は削減されている。

第２２実施例は入出力用の楕円曲線としてワイエルシュトラス型楕円曲線を、内部の計算用には与えられたワイエルシュトラス型楕円曲線から変換可能であるモンゴメリ型楕円曲線を用いたものである。スカラー倍計算部１０３が、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、ワイエルシュトラス型楕円曲線におけるアフィン座標の点として完全な座標が与えられたスカラー倍点$(x_d^W, y_d^W)$を計算し出力する。スカラー値d及びワイエルシュトラス型楕円曲線上の点Pをスカラー倍計算部１０３に入力すると高速スカラー倍計算部２０２がそれを受け取る。高速スカラー倍計算部２０２は受け取ったスカラー値dと与えられたワイエルシュトラス型楕円曲線上の点Pからモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$を計算し、アフィン座標で表された入力されたモンゴメリ型楕円曲線上の点$P=(x, y)$と共にその情報を座標復元部２０３に与える。座標復元部２０３は与えられた座標の値$x_d$、$x_{d+1}$、x及びyよりワイエルシュトラス型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d^W, y_d^W)$の座標$y_d^W$の復元を行なう。スカラー倍計算部１０３はワイエルシュトラス型楕円曲線上でアフィン座標において完全に座標が与えられたスカラー倍点$(x_d^W, y_d^W)$を計算結果として出力する。

次に図４２により、座標x、y、$x_d$、$x_{d+1}$が与えられた場合に、$x_d^W$、$y_d^W$を出力する座標復元部の処理について説明する。

座標復元部２０３では、モンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点$dP=(x_d, y_d)$の座標のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点$(d+1)P=(x_{d+1}, y_{d+1})$の座標のうち$x_{d+1}$、スカラー倍計算部１０３に入力されたモンゴメリ型楕円曲線上の点Pをアフィン座標で表した$(x, y)$を入力し、以下の手順でアフィン座標において完全な座標が与えられたスカラー倍点$(x_d^W, y_d^W)$を出力する。

ステップ４２０１において$x_d \times x$が計算され、レジスタ$T_1$に格納される。ステップ４２０２において$T_1+1$が計算される。ここでレジスタ$T_1$には$x_d x$が格納されており、したがって$x_d x+1$が計算される。その結果がレジスタ$T_1$に格納

される。ステップ４２０３において$x_d$+xが計算され、レジスタ$T_2$に格納される。ステップ４２０４において$T_2$+2Aが計算される。ここでレジスタ$T_2$には$x_d$+xが格納されており、したがって$x_d$+x+2Aが計算される。その結果がレジスタ$T_2$に格納される。ステップ４２０５において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$x_d x+1$がレジスタ$T_2$には$x_d+x+2A$がそれぞれ格納されており、したがって$(x_d x+1)(x_d+x+2A)$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４２０６において$T_1$-2Aが計算される。ここでレジスタ$T_1$には$(x_d x+1)(x_d+x+2A)$が格納されており、したがって$(x_d x+1)(x_d+x+2A)-2A$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４２０７において$x_d$-xが計算され、レジスタ$T_2$に格納される。ステップ４２０８において$T_2$の２乗が計算される。ここでレジスタ$T_2$には$x_d$-xが格納されており、したがって$(x_d-x)^2$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４２０９において$T_2 \times x_{d+1}$が計算される。ここでレジスタ$T_2$には$(x_d-x)^2$が格納されており、したがって$(x_d-x)^2 x_{d+1}$が計算される。その結果がレジスタ$T_2$に格納される。ステップ４２１０において$T_1-T_2$が計算される。ここでレジスタ$T_1$には$(x_d x+1)(x_d+x+2A)-2A$がレジスタ$T_2$には$(x_d-x)^2 x_{d+1}$がそれぞれ格納されており、したがって$(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４２１１において2B×yが計算され、レジスタ$T_2$に格納される。ステップ４２１２において$T_2$の逆元が計算される。ここでレジスタ$T_2$には2Byが格納されており、したがって1/2Byが計算される。その結果がレジスタ$T_2$に格納される。ステップ４２１３において$T_1 \times T_2$が計算される。ここでレジスタ$T_1$には$(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}$がレジスタ$T_2$には1/2Byがそれぞれ格納されており、したがって$\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2By$が計算される。その結果がレジスタ$T_1$に格納される。ステップ４２１４において$T_1 \times (1/s)$が計算される。ここでレジスタ$T_1$には$\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2By$が格納されており、したがって$\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2Bys$が計算される。その結果がレジスタ$y_d^W$に格納される。ステップ４２１５において$x_d \times (1/s)$が計算され、レジスタ$T_1$に格納される。ステ

ップ４２１６において$T_1+\alpha$が計算される。ここでレジスタ$T_1$には$x_d/s$が格納されており、したがって$(x_d/s)+\alpha$が計算される。その結果がレジスタ$x_d^W$に格納される。したがってレジスタ$x_d^W$には$(x_d/s)+\alpha$が格納されている。レジスタ$y_d^W$はステップ４２１４において$\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/2Bys$が格納され、その後更新されないので、その値が保持されている。

上記手順によりスカラー倍点のy座標$y_d$が復元される理由は以下の通りである。点(d+1)Pは点dPに点Pを加算した点である。モンゴメリ型楕円曲線のアフィン座標における加算公式に代入すると、数６を得る。点P及び点dPはモンゴメリ型楕円曲線上の点であるので、$By_d^2=x_d^3+Ax_d^2+x_d$及び$By^2=x^3+Ax^2+x$をみたす。数６に代入し、$By_d^2$及び$By^2$を消去し、式を整理すると、数６４を得る。モンゴメリ型楕円曲線上の点とワイエルシュトラス型楕円曲線上の点との対応関係については、K. Okeya, H. Kurumatani, K. Sakurai, Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications, Public Key Cryptography, LNCS 1751 (2000) pp. 238-257 に記載されている。それによると、変換パラメタをs, αとして、$y_d^W=s^{-1}y_d$及び$x_d^W=s^{-1}x_d+\alpha$の関係がある。結果として数８７、数６３を得る。

$$y_d^W=\{(x_d x+1)(x_d+x+2A)-2A-(x_d-x)^2 x_{d+1}\}/(2sBy) \quad \cdots 数８７$$

ここで、$x_d^W$, $y_d^W$は図４２により与えられる。したがって、アフィン座標$(x_d^W, y_d^W)$の値は全て復元されていることになる。

上記手順はステップ４２０１、ステップ４２０５、ステップ４２０９、ステップ４２１１、ステップ４２１３、ステップ４２１４及びステップ４２１５において有限体上の乗算の計算量を必要とする。また、ステップ４２０８において有限体上の２乗算の計算量を必要とする。さらにステップ４２１２において有限体上の逆元演算の計算量を必要とする。有限体上の加算及び減算の計算量は、有限体上の乗算の計算量、２乗算の計算量、逆元演算の計算量と比べて比較的小さいので無視してもよい。有限体上の乗算の計算量をM、有限体上の２乗算の計算量をS、有限体上の逆元演算の計算量をＩとすると、上記手順は７Ｍ＋Ｓ＋Ｉの計算量を必要とする。これは高速スカラー倍計算の計算量と比べてはるかに小さい。例えばスカラー値dが１６０ビットであれば、高速スカラー倍計算の計算量はお

およそ１５００M弱と見積もられる。Ｓ＝０．８M及びＩ＝４０Mと仮定すると座標復元の計算量は４７．８Mであり、高速スカラー倍計算の計算量と比べてはるかに小さい。したがって効率的に座標を復元できていることが示された。

尚、上記手順をとらなくても、上記等式の右辺の値が計算できれば$y_d{}^W$の値が復元できる。その場合は一般的に復元に必要となる計算量が増大する。また、楕円曲線のパラメータであるA乃至はBやモンゴメリ型楕円曲線への変換パラメータsの値を小さくとることにより、ステップ４２０６、ステップ４２１１、ステップ４２１４乃至はステップ４２１５における乗算の計算量を削減することができる。

次に図４５により、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$，$x_{d+1}$を出力する高速スカラー倍計算部の処理について説明する。高速スカラー倍計算部２０２では、スカラー倍計算部１０３に入力されたワイエルシュトラス型楕円曲線上の点Pを入力し、以下の手順によりモンゴメリ型楕円曲線においてアフィン座標で表されたスカラー倍点dP=($x_d$, $y_d$)のうち$x_d$、アフィン座標で表されたモンゴメリ型楕円曲線上の点(d+1)P=($x_{d+1}$, $y_{d+1}$)のうち$x_{d+1}$を出力する。ステップ４５１６として、与えられたワイエルシュトラス型楕円曲線上の点Pをモンゴメリ型楕円曲線上で射影座標により表された点に変換する。この点をあらためて点Pとする。ステップ４５０１として、変数Ｉに初期値１を代入する。ステップ４５０２として、点Pの２倍点2Pを計算する。ここで点Pは射影座標において(x, y, 1)として表し、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて２倍点2Pを計算する。ステップ４５０３として、スカラー倍計算部１０３に入力された楕円曲線上の点Pとステップ４５０２で求めた点2Pを、点の組(P, 2P)として格納する。ここで点P及び点2Pは射影座標で表されている。ステップ４５０４として、変数Ｉとスカラー値dのビット長とが一致するかどうかを判定し、一致すればステップ４５１５へ行く。一致しなければステップ４５０５へ行く。ステップ４５０５として、変数Ｉを１増加させる。ステップ４５０６として、スカラー値のＩ番目のビットの値が０であるか１であるかを判定する。そのビットの値が０であればステップ４５０７へ行く。そのビットの値が１であればステップ４５１０へ行く。ステップ４５０７として、射影座

標により表された点の組(mP, (m+1)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ４５０８へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４５０８として、射影座標により表された点の組(mP, (m+1)P)から点mPの２倍算2(mP)を行ない、点2mPを計算する。その後ステップ４５０９へ行く。ここで、２倍算2(mP)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４５０９として、ステップ４５０８で求めた点2mPとステップ４５０７で求めた点(2m+１)Pを点の組(2mP, (2m+１)P)として、点の組(mP, (m+１)P)の代わりに格納する。その後ステップ４５０４へ戻る。ここで、点2mP、点(2m+1)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ４５１０として、射影座標により表された点の組(mP, (m+１)P)から点mPと点(m+1)Pの加算mP+(m+1)Pを行ない、点(2m+1)Pを計算する。その後ステップ４５１１へ行く。ここで、加算mP+(m+1)Pは、モンゴメリ型楕円曲線の射影座標における加算公式を用いて計算される。ステップ４５１１として、射影座標により表された点の組(mP, (m+１)P)から点(m+１)Pの２倍算2((m+１)P)を行ない、点(2m+2)Pを計算する。その後ステップ４５１２へ行く。ここで、２倍算2((m+１)P)は、モンゴメリ型楕円曲線の射影座標における２倍算の公式を用いて計算される。ステップ４５１２として、ステップ４５１０で求めた点(2m+１)Pとステップ４５１１で求めた点(2m+2)Pを点の組((2m+１)P, (2m+2)P)として、点の組(mP, (m+1)Pの代わりに格納する。その後ステップ４５０４へ戻る。ここで、点(2m+１)P、点(2m+2)P、点mP及び点(m+1)Pは全て射影座標において表されている。ステップ４５１５として、射影座標で表された点mP=$(X_m, Y_m, Z_m)$より$X_m$及び$Z_m$をそれぞれ$X_d$及び$Z_d$とし、射影座標で表された点(m+1)P＝$(X_{m+1}, Y_{m+1}, Z_{m+1})$より$X_{m+1}$及び$Z_{m+1}$をそれぞれ$X_{d+1}$及び$Z_{d+1}$とする。ここで、$Y_m$及び$Y_{m+1}$は、モンゴメリ型楕円曲線の射影座標における加算公式及び２倍算の公式ではY座標を求める事ができないので、求まっていない。$X_d$，$Z_d$，$X_{d+1}$，$Z_{d+1}$より、$x_d=X_d Z_{d+1}/Z_d Z_{d+1}$，$x_{d+1}=Z_d X_{d+1}/Z_d Z_{d+1}$として$x_d$，$x_{d+1}$を求める。その後ステップ４５１３へ行く。ステップ４５１３として、$x_d$，$x_{d+1}$を出力する。上記手順により、mとスカラー値dはビット長が等しく

さらにそのビットのパターンも同じとなる為、等しくなる。

モンゴメリ型楕円曲線の射影座標における加算公式の計算量は、$Z_1=1$ととることにより３Ｍ＋２Ｓとなる。ここでMは有限体上の乗算の計算量、Ｓは有限体上の２乗算の計算量である。モンゴメリ型楕円曲線の射影座標における２倍算の公式の計算量は、３Ｍ＋２Ｓである。スカラー値のＩ番目のビットの値が０であれば、ステップ４５０７において加算の計算量、ステップ４５０８において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要となる。スカラー値のＩ番目のビットの値が１であれば、ステップ４５１０において加算の計算量、ステップ４５１１において２倍算の計算量が必要となる。すなわち６Ｍ＋４Ｓの計算量が必要である。いずれの場合においても６Ｍ＋４Ｓの計算量が必要である。ステップ４５０４、ステップ４５０５、ステップ４５０６、ステップ４５０７、ステップ４５０８、ステップ４５０９乃至はステップ４５０４、ステップ４５０５、ステップ４５０６、ステップ４５１０、ステップ４５１１、ステップ４５１２の繰り返しの回数は、（スカラー値dのビット長）－１回となるので、ステップ４５０２での２倍算の計算量及びステップ４５１５でのアフィン座標への変換の計算量を考慮に入れると、全体の計算量は（６Ｍ＋４Ｓ）ｋ＋３Ｍ－２Ｓ＋Ｉとなる。ここでｋはスカラー値dのビット長である。一般的には、計算量Ｓは、Ｓ＝０．８Ｍ程度、計算量ＩはＩ＝４０Ｍ程度と見積もられるので、全体の計算量はおおよそ（９．２ｋ＋４１．４）Ｍとなる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、上記手順のアルゴリズムの計算量はおおよそ１５１３Ｍとなる。スカラー値dのビットあたりの計算量としてはおよそ９．２Ｍとなる。A. Miyaji, T. Ono, H. Cohen, Efficient elliptic curve exponentiation using mixed coordinates, Advances in Cryptology Proceedings of ASIACRYPT'98, LNCS 1514 (1998) pp. 51-65 には、ワイエルシュトラス型楕円曲線において、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法は高速なスカラー倍計算方法として記載されている。この場合においては、スカラー値のビットあたりの計算量はおおよそ１０Ｍと見積もられ、これ以外にアフィン座標への変換の計算量が必要となる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算方法の計算

量はおおよそ１６４０Ｍとなる。したがって、上記手順のアルゴリズムの方が計算量が少なく高速といえる。

尚、高速スカラー倍計算部２０２において上記手順のアルゴリズムを用いなくても、スカラー値d及びワイエルシュトラス型楕円曲線上の点Pから、$x_d$, $x_{d+1}$を出力するアルゴリズムであり且つ高速であれば、他のアルゴリズムを用いていもよい。

スカラー倍計算部１０３における座標復元部２０３の座標復元に必要な計算量は７Ｍ＋Ｓ＋Ｉであり、これは高速スカラー倍計算部２０２の高速スカラー倍計算に必要な計算量の（９．２ｋ＋４１．４）Ｍとに比べてはるかに小さい。したがって、スカラー倍計算部１０３のスカラー倍計算に必要な計算量は、高速スカラー倍計算部の高速スカラー倍計算に必要な計算量とほぼ同等である。Ｉ＝４０Ｍ、Ｓ＝０．８Ｍと仮定すると、この計算量はおおよそ（９．２ｋ＋８９．２）Ｍと見積もることができる。例えばスカラー値dが１６０ビット（ｋ＝１６０）であれば、このスカラー倍計算に必要な計算量は１５６１Ｍとなる。楕円曲線としてワイエルシュトラス型楕円曲線を使用し、ウィンドウ法を用いてヤコビアン座標を中心とした混合座標系を用いたスカラー倍計算方法を用いて、スカラー倍点をアフィン座標として出力する場合に必要となる計算量はおおよそ１６４０Ｍであり、これと比べて必要となる計算量は削減されている。

以上、図１に示した暗号／復号処理装置を復号化処理を行う装置として第１から第２２の実施例を説明したが、同様に暗号化処理を行う装置としても利用できる。その場合には、既に説明したように暗号／復号処理装置のスカラー倍計算部１０３は、既に説明した楕円曲線上の点Ｑ、乱数ｋによるスカラー倍点と、公開鍵ａＱと乱数ｋによるスカラー倍点を出力する。このとき、実施例１から２２で説明したスカラー値dを乱数ｋ、楕円曲線上の点Ｐを楕円曲線上の点Ｑ、公開鍵ａＱとして同様の処理を行うことにより、それぞれのスカラー倍点を求めることができる。

尚、図１に示した暗号／復号処理装置は、暗号化、復号化の両方を行えるように示したが、暗号化の処理のみ、あるいは復号化の処理のみを行えるように構成してもよい。

また、第１から第２２の実施例で説明した処理については、コンピュータ読み取り可能な記憶媒体に格納されたプログラムであってもよい。この場合は、そのプログラムを図１の記憶部へ読み込み、処理部であるＣＰＵなどの演算装置がこのプログラムに従って、処理を行う。

図２７は、図１の暗号処理システムにおける秘密情報を用いた暗号処理において、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法の実施例を示す図である。図３３は、図２７のスカラー倍計算方法の実施例における処理の流れを示すフローチャートである。

図３３において、図２７のスカラー倍計算部２７０１は以下のようにして、スカラー値及びワイエルシュトラス型楕円曲線上の点から、ワイエルシュトラス型楕円曲線上で完全な座標が与えられたスカラー倍点を計算し出力する。スカラー値及びワイエルシュトラス型楕円曲線上の点をスカラー倍計算部２７０１に入力すると、楕円曲線変換部２７０４がワイエルシュトラス型楕円曲線上の点をモンゴメリ型楕円曲線上の点に変換する。（ステップ３３０１）。高速スカラー倍計算部２７０２はスカラー倍計算部２７０１に入力されたスカラー値及び楕円曲線変換部２７０４が変換したモンゴメリ型楕円曲線上の点を受け取る（ステップ３３０２）。高速スカラー倍計算部２７０２は受け取ったスカラー値とモンゴメリ型楕円曲線上の点からモンゴメリ型楕円曲線上のスカラー倍点の座標の一部の値を計算し（ステップ３３０３）、その情報を座標復元部２７０３に与える（ステップ３３０４）。座標復元部２７０３は与えられたモンゴメリ型楕円曲線上のスカラー倍点の情報及び楕円曲線変換部２７０４により変換されたモンゴメリ型楕円曲線上の点よりモンゴメリ型楕円曲線上のスカラー倍点の座標の復元を行なう（ステップ３３０５）。楕円曲線逆変換部２７０５は、座標復元部２７０３により復元されたモンゴメリ型楕円曲線上のスカラー倍点をワイエルシュトラス型楕円曲線上のスカラー倍点に変換する（ステップ３３０６）。スカラー倍計算部２７０１はワイエルシュトラス型楕円曲線上で完全に座標が与えられたスカラー倍点を計算結果として出力する。（ステップ３３０７）。

スカラー倍計算部２７０１における高速スカラー倍計算部２７０２及び座標復元部２７０３が実行するモンゴメリ型楕円曲線上のスカラー倍計算は、上述した

第１～第５及び第１４～第１６実施例で説明したモンゴメリ型楕円曲線上におけるスカラー倍計算方法がそのまま適応される。したがってこのスカラー倍計算は、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法である。

図２２は、図１の本実施形態の暗号処理システムを署名作成装置として利用する場合の構成を示す。図１の暗号処理部１０２は、図２２の署名作成装置２２０１では署名部２２０２になる。図２８は、図２２の署名作成装置における処理の流れを示すフローチャートである。図２９は、図２２の署名作成装置における処理の流れを示すシーケンス図である。

図２８において、署名作成装置２２０１は以下のようにして、与えられたメッセージ２２０５から署名が付随しているメッセージ２２０６を出力する。メッセージ２２０５を署名作成装置２２０１に入力すると署名部２２０２がそれを受け取る（ステップ２８０１）。署名部２２０２はスカラー倍計算部２２０３に受け取ったメッセージ２２０５に応じて楕円曲線上の点を与える（ステップ２８０２）。スカラー倍計算部２２０３は秘密情報格納部２２０４より秘密情報であるスカラー値を受け取る（ステップ２８０３）。スカラー倍計算部２２０３は受け取った楕円曲線上の点とスカラー値よりスカラー倍点を計算し（ステップ２８０４）、そのスカラー倍点を署名部２２０２に送る（ステップ２８０５）。署名部２２０２はスカラー倍計算部２２０３より受け取ったスカラー倍点をもとにして署名作成処理を行なう（ステップ２８０６）。その結果を署名が付随したメッセージ２２０６として出力する（ステップ２８０７）。

上記処理手順を図２９のシーケンス図を用いて説明する。まず、署名部２９０１（図２２の２２０２）の実行する処理について説明する。署名部２９０１は、入力メッセージを受け取る。署名部２９０１は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部２９０２に楕円曲線上の点を与え、そしてスカラー倍計算部２９０２からスカラー倍点を受け取る。署名部２９０１は、受け取ったスカラー倍点を用いて署名作成処理を行ない、その結果を出力メッセージとして出力する。

次にスカラー倍計算部２９０２（図２２の２２０３）の実行する処理について説明する。スカラー倍計算部２９０２は、署名部２９０１より楕円曲線上の点を

受け取る。スカラー倍計算部２９０２は、秘密情報格納部２９０３よりスカラー値を受け取る。スカラー倍計算部２９０２は、受け取った楕円曲線上の点及びスカラー値から、完全な座標を与え且つ高速なスカラー倍計算方法により、スカラー倍点を計算し、署名部２９０１にスカラー倍点を送る。

最後に秘密情報格納部２９０３（図２２の２２０４）の実行する処理について説明する。秘密情報格納部２９０３は、スカラー倍計算部２９０２がスカラー倍を計算できるように、スカラー値をスカラー倍計算部２９０２に送る。

スカラー倍計算部２２０３が実行するスカラー倍計算は、上述した第１～第２２実施例で説明したものがそのまま適応される。したがってこのスカラー倍計算は、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法である。そのため署名部２２０２において、署名作成処理を行なう際に、スカラー倍点の完全な座標を用いることができ、その上高速に実行できる。

図２３は、図１の本実施形態の暗号処理システムを復号化装置として利用する場合の構成を示す。図１の暗号処理部１０２は、図２３の復号化装置２３０１では復号部２３０２になる。図３０は、図２３の復号化装置における処理の流れを示すフローチャートである。図３１は、図２３の復号化装置における処理の流れを示すシーケンス図である。

図３０において、復号装置２３０１は以下のようにして、与えられたメッセージ２３０５から復号化されたメッセージ２３０６を出力する。メッセージ２３０５を復号装置２３０１に入力すると復号部２３０２がそれを受け取る（ステップ３００１）。復号部２３０２はスカラー倍計算部２３０３に受け取ったメッセージ２３０５に応じて楕円曲線上の点を与える（ステップ３００２）。スカラー倍計算部２３０３は秘密情報格納部２３０４より秘密情報であるスカラー値を受け取る（ステップ３００３）。スカラー倍計算部２３０３は受け取った楕円曲線上の点とスカラー値よりスカラー倍点を計算し（ステップ３００４）、そのスカラー倍点を復号部２３０２に送る（ステップ３００５）。復号部２３０２はスカラー倍計算部２３０３より受け取ったスカラー倍点をもとにして復号化処理を行なう（ステップ３００６）。その結果を復号化されたメッセージ２３０６として出力する（ステップ３００７）。

上記処理手順を図３１のシーケンス図を用いて説明する。まず、復号化部３１０１（図２３の２３０２）の実行する処理について説明する。復号化部３１０１は、入力メッセージを受け取る。復号化部３１０１は、入力メッセージをもとに楕円曲線上の点を選び、スカラー倍計算部３１０２に楕円曲線上の点を与え、そしてスカラー倍計算部３１０２からスカラー倍点を受け取る。復号化部３１０１は、受け取ったスカラー倍点を用いて復号化処理を行ない、その結果を出力メッセージとして出力する。

次にスカラー倍計算部３１０２（図２３の２３０３）の実行する処理について説明する。スカラー倍計算部３１０２は、復号化部３１０１より楕円曲線上の点を受け取る。スカラー倍計算部３１０２は、秘密情報格納部３１０３よりスカラー値を受け取る。スカラー倍計算部３１０２は、受け取った楕円曲線上の点及びスカラー値から、完全な座標を与え且つ高速なスカラー倍計算方法により、スカラー倍点を計算し、復号化部３１０１にスカラー倍点を送る。

最後に秘密情報格納部３１０３（図２３の２３０４）の実行する処理について説明する。秘密情報格納部３１０３は、スカラー倍計算部３１０２がスカラー倍を計算できるように、スカラー値をスカラー倍計算部３１０２に送る。

スカラー倍計算部２３０３が実行するスカラー倍計算は、上述した第１～第２２実施例で説明したものがそのまま適応される。したがってこのスカラー倍計算は、スカラー倍点の完全な座標を与え且つ高速なスカラー倍計算方法である。そのため復号部２３０２において、復号化処理を行なう際に、スカラー倍点の完全な座標を用いることができ、その上高速に実行できる。

以上述べたように本発明によれば、暗号処理システムにおける秘密情報を用いた暗号処理において用いられるスカラー倍計算が高速化されており、暗号処理の高速化が計れる。また、スカラー倍点の座標を完全に与えることができるので、全ての暗号処理を行なうことができる。

# 請 求 の 範 囲

1. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有するスカラー倍計算方法。

2. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報からアフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

3. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から射影座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

4. 楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有するスカラー倍計算方法。

5. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報から完全な座標を復元するステップとを有するスカラー倍計算方法。

6. 楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円円

曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、 前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

7. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

8. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

9. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点の射影座標における

X座標及びZ座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

10. 楕円曲線暗号における標数5以上の有限体上定義されたモンゴメリ型楕円曲線において、スカラー値及びモンゴメリ型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点のx座標、前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるx座標並びに前記スカラー倍点と前記モンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるx座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

11. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

12. 楕円曲線暗号における標数5以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報として射影座標で与えられた前記スカラー倍点のX座標及びZ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、射影

座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

13. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記スカラー倍点の部分情報を計算するステップと、前記スカラー倍点の部分情報としてアフィン座標で与えられた前記スカラー倍点のｘ座標、前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を加算した点のアフィン座標におけるｘ座標並びに前記スカラー倍点と前記ワイエルシュトラス型楕円曲線上の点を減算した点のアフィン座標におけるｘ座標を与え、アフィン座標において完全な座標を復元するステップとを有するスカラー倍計算方法。

14. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からワイエルシュトラス型楕円曲線において完全な座標を復元するステップとを有するスカラー倍計算方法。

15. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からモンゴメリ型楕円曲線において完全な座標を復元するステップと、前記モンゴメリ型楕円曲線において完全な座標が復元されたスカラー倍点からワイエルシュトラス型楕円曲線におけるスカラー倍点を計算するステップとを有するスカラー倍計算方法。

16. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点か

らスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

17. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

18. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のX座標及びZ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるX座標及びZ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるX座標及びZ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有する

スカラー倍計算方法。

19. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線において射影座標で与えられたスカラー倍点のＸ座標及びＺ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点の射影座標におけるＸ座標及びＺ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点の射影座標におけるＸ座標及びＺ座標を与え、ワイエルシュトラス型楕円曲線において射影座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

20. 楕円曲線暗号における標数５以上の有限体上定義されたワイエルシュトラス型楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算方法であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換するステップと、モンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算するステップと、前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報としてモンゴメリ型楕円曲線においてアフィン座標で与えられたスカラー倍点のｘ座標、前記スカラー倍点とモンゴメリ型楕円曲線上の点を加算した点のアフィン座標におけるｘ座標並びに前記スカラー倍点とモンゴメリ型楕円曲線上の点を減算した点のアフィン座標におけるｘ座標を与え、ワイエルシュトラス型楕円曲線においてアフィン座標における完全な座標を復元するステップとを有するスカラー倍計算方法。

21. 第１のデータから第２のデータを生成するデータ生成方法であって、請求項１から２０の何れか一つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とするデータ生成方法。

22. データから署名データを生成する署名生成方法であって、請求項１から２

０の何れか一つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする署名生成方法。

23. 暗号化されたデータから復号化されたデータを生成する復号化方法であって、請求項１から２０の何れか一つに記載のスカラー倍計算方法を用いてスカラー倍を計算するステップを有することを特徴とする復号化方法。

24. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及び楕円曲線上の点からスカラー倍点を計算するスカラー倍計算部であって、

前記スカラー倍点の部分情報を計算する高速スカラー倍計算部と、前記スカラー倍点の部分情報から完全な座標を復元する座標復元部とを有し、

前記スカラー倍計算部は、高速スカラー倍計算部により前記スカラー倍点の部分情報を計算した後、座標復元部により前記スカラー倍点の部分情報から完全な座標を復元し、スカラー倍点を計算することを特徴とする。

25. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、スカラー値及びワイエルシュトラス型楕円曲線上の点からスカラー倍点を計算するスカラー倍計算部であって、

前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換する楕円曲線変換部と、前記スカラー倍点の部分情報を計算する高速スカラー倍計算部と、前記スカラー倍点の部分情報から完全な座標を復元する座標復元部と、モンゴメリ型楕円曲線をワイエルシュトラス型楕円曲線に変換する楕円曲線逆変換部とを有し、

前記スカラー倍計算部は、楕円曲線変換部により前記ワイエルシュトラス型楕円曲線をモンゴメリ型楕円曲線に変換し、高速スカラー倍計算部によりモンゴメリ型楕円曲線におけるスカラー倍点の部分情報を計算し、座標復元部により前記モンゴメリ型楕円曲線におけるスカラー倍点の部分情報からモンゴメリ型楕円曲線において完全な座標を復元し、楕円曲線逆変換部によりモンゴメリ型楕円曲線において完全な座標が復元されたスカラー倍点からワイエルシュトラス型楕円曲線におけるスカラー倍点を計算し、スカラー倍点を計算することを特徴とする。

26. 請求項１から２０の何れか一つに記載のスカラー倍計算方法に係るプログ

ラムを格納したことを特徴とする記憶媒体。

27. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、不完全な座標で与えられた楕円曲線上の点から完全な座標を復元する座標復元方法であって、

前記不完全な座標を持つ点及び前記不完全な座標を持つ点と完全な座標を持つ点との加算及び減算によって得られる点により、前記不完全な座標を持つ点の座標を計算するステップを有する座標復元方法。

28. 楕円曲線暗号における標数５以上の有限体上定義された楕円曲線において、不完全な座標で与えられた楕円曲線上の点から完全な座標を復元する座標復元方法であって、

前記不完全な座標を持つ点及び前記不完全な座標を持つ点と完全な座標を持つ点との加算によって得られる点から、前記不完全な座標を持つ点と完全な座標を持つ点との減算によって得られる点を計算するステップと、前記不完全な座標を持つ点の座標を計算するステップを有する座標復元方法。

29. 楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、不完全な座標で与えられたモンゴメリ型楕円曲線上の点からワイエルシュトラス型楕円曲線において完全な座標を復元する座標復元方法であって、

前記モンゴメリ型楕円曲線において不完全な座標を持つ点及び前記モンゴメリ型楕円曲線において不完全な座標を持つ点と完全な座標を持つ点との加算及び減算によって得られる点から、前記モンゴメリ型楕円曲線において不完全な座標を持つ点の座標を計算するステップと、前記完全な座標が計算されたモンゴメリ型楕円曲線の点をワイエルシュトラス型楕円曲線の点に変換するステップとを有する座標復元方法。

30. 楕円曲線暗号における標数５以上の有限体上定義されたモンゴメリ型楕円曲線において、不完全な座標で与えられたモンゴメリ型楕円曲線上の点からワイエルシュトラス型楕円曲線において完全な座標を復元する座標復元方法であって、

前記モンゴメリ型楕円曲線において不完全な座標を持つ点及び前記モンゴメリ型楕円曲線において不完全な座標を持つ点と完全な座標を持つ点との加算によって得られる点から、前記モンゴメリ型楕円曲線において不完全な座標を持つ点と

完全な座標を持つ点との減算によって得られる点を計算するステップと、前記モンゴメリ型楕円曲線において不完全な座標を持つ点の座標を計算するステップと、前記完全な座標が計算されたモンゴメリ型楕円曲線の点をワイエルシュトラス型楕円曲線の点に変換するステップとを有する座標復元方法。

FIG. 1

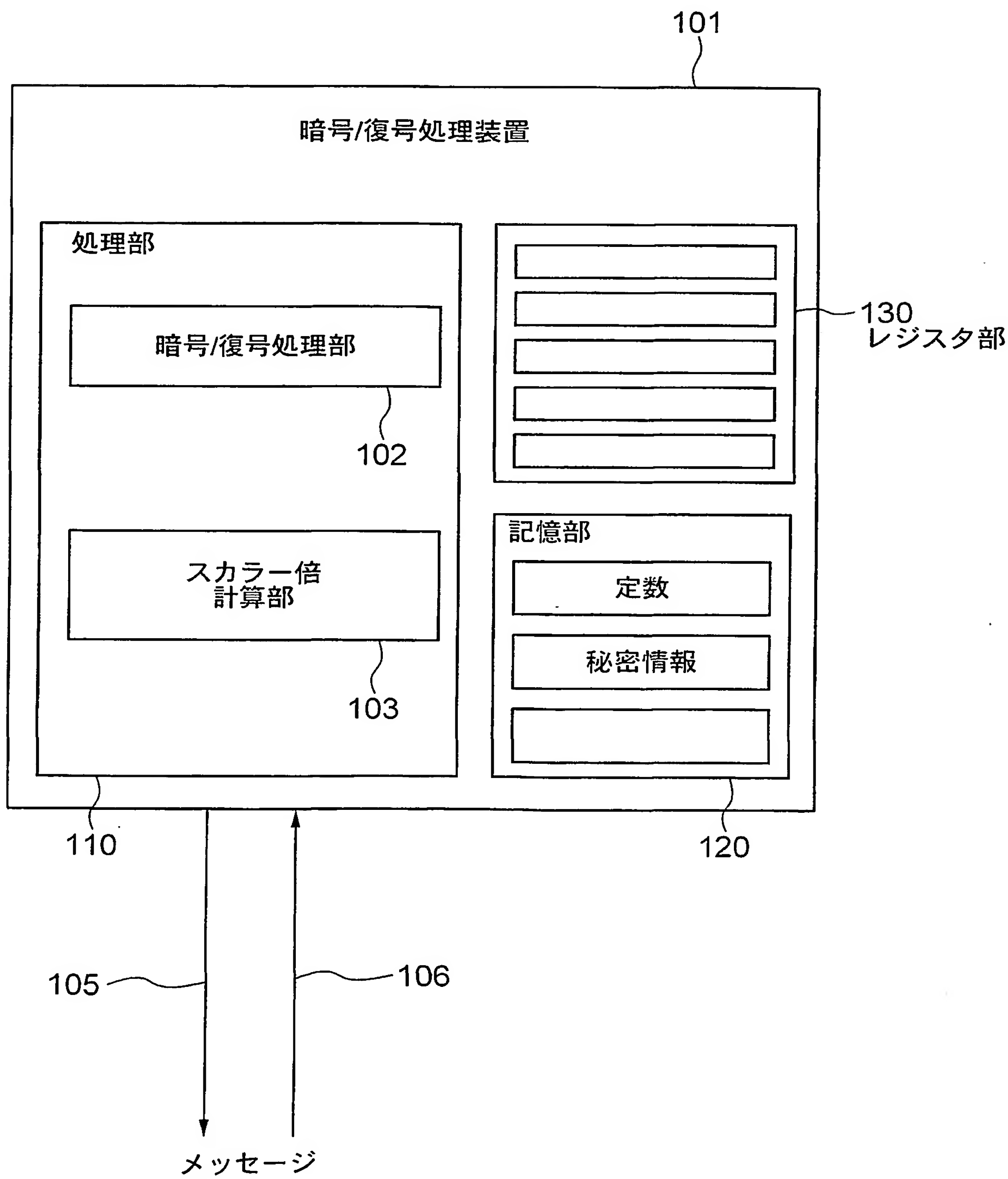

101
暗号/復号処理装置
処理部
暗号/復号処理部
102
スカラー倍
計算部
103
130
レジスタ部
記憶部
定数
秘密情報
110
120
105
106
メッセージ

FIG. 2

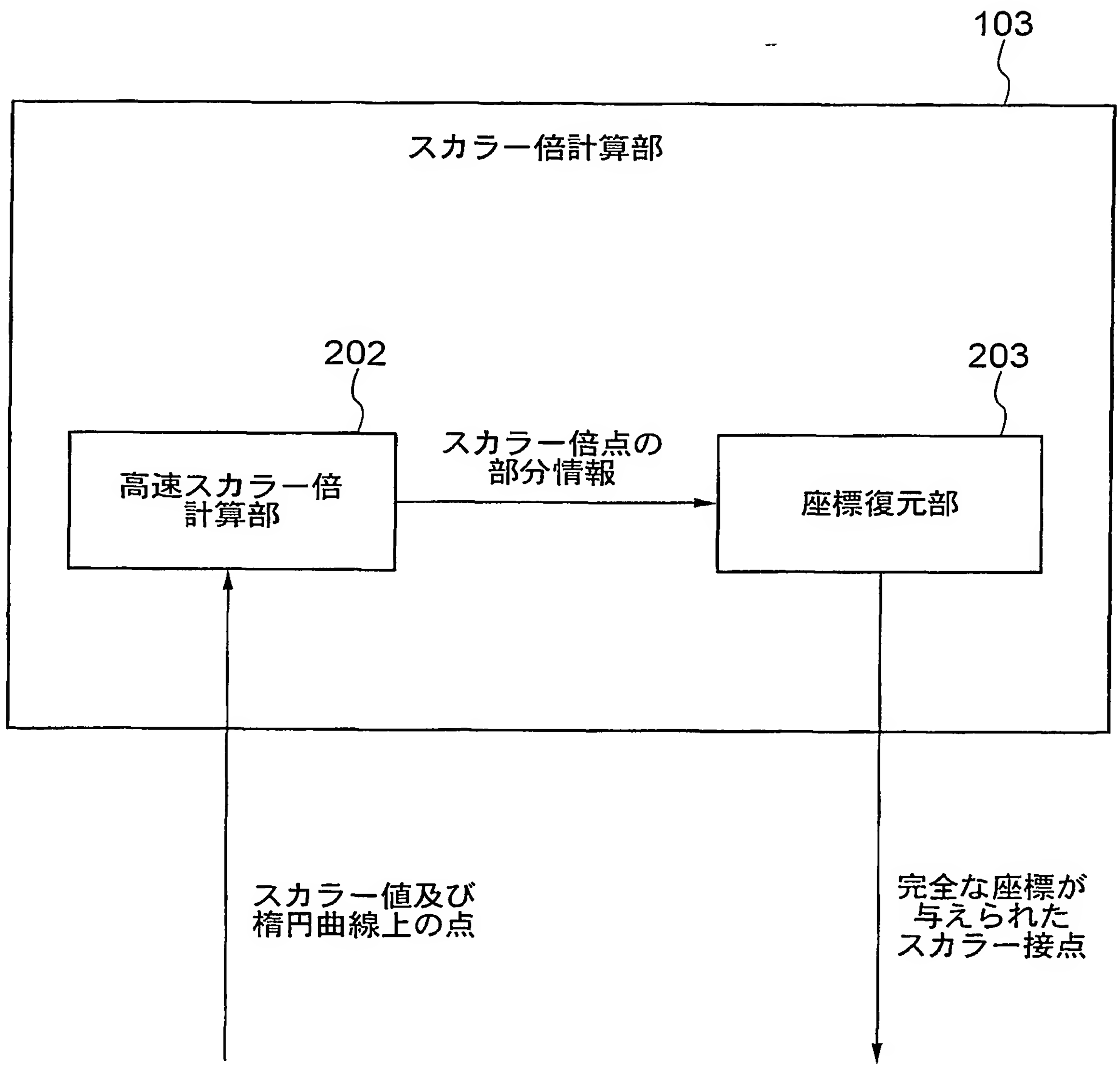

103
スカラー倍計算部
202
高速スカラー倍計算部
スカラー倍点の部分情報
203
座標復元部
スカラー値及び楕円曲線上の点
完全な座標が与えられたスカラー接点

FIG. 3

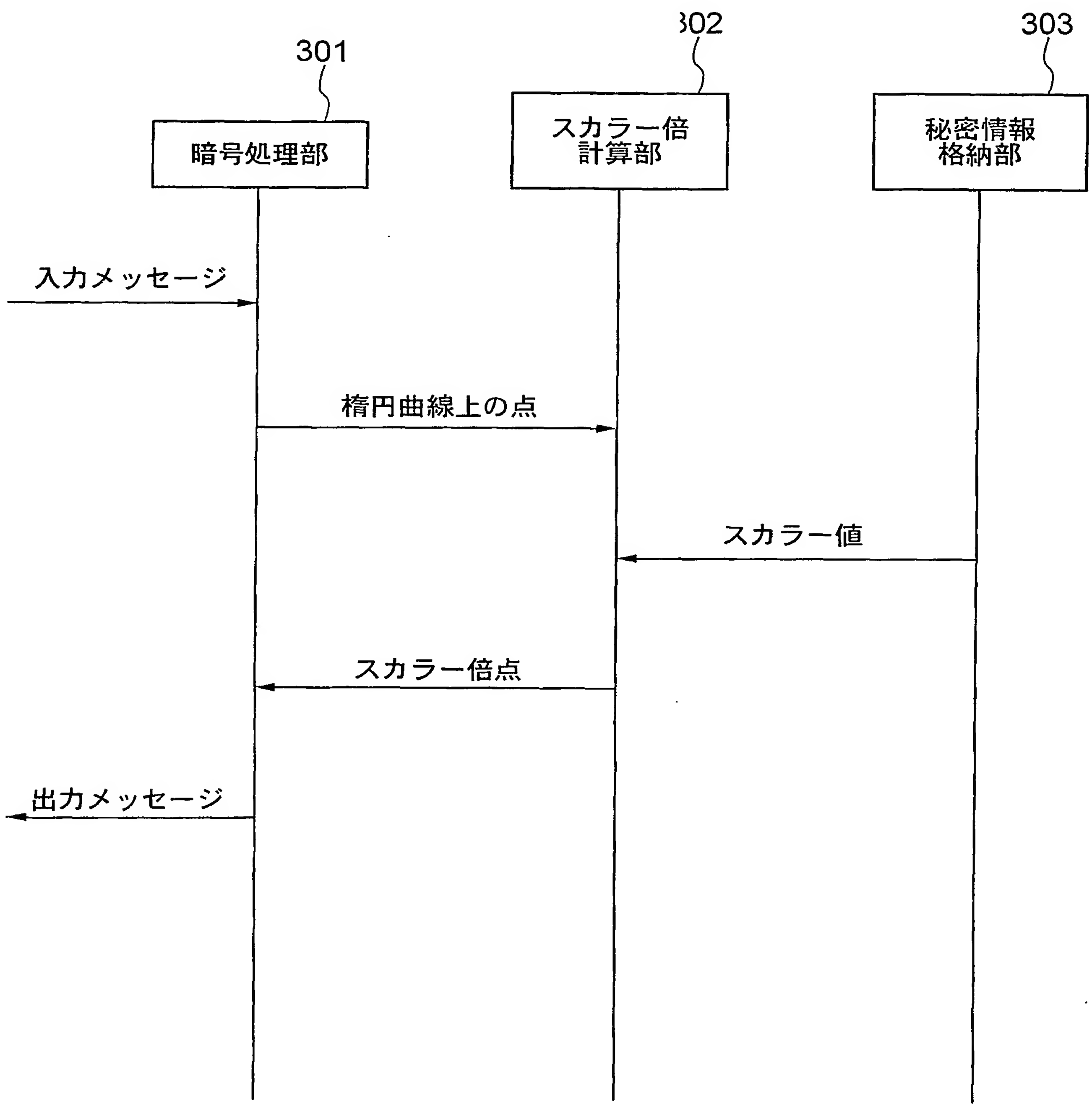

302
303
301
暗号処理部
スカラー倍
計算部
秘密情報
格納部
入力メッセージ
楕円曲線上の点
スカラー値
スカラー倍点
出力メッセージ

FIG. 4

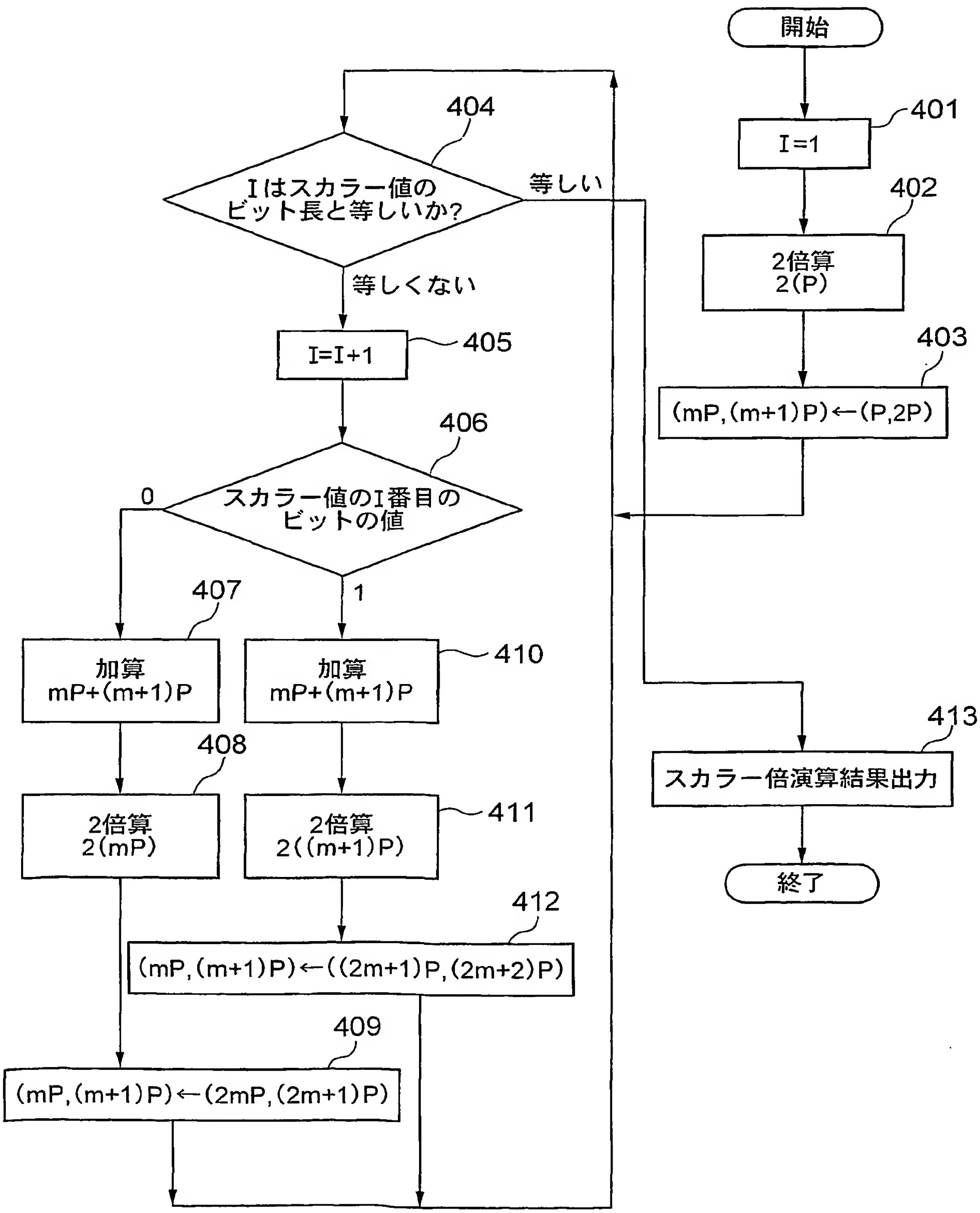

開始
I=1
401
2倍算
2(P)
402
(mP,(m+1)P)←(P,2P)
403
404
Iはスカラー値のビット長と等しいか?
等しい
等しくない
I=I+1
405
406
スカラー値のI番目のビットの値
0
1
加算
mP+(m+1)P
407
加算
mP+(m+1)P
410
2倍算
2(mP)
408
2倍算
2((m+1)P)
411
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
412
(mP,(m+1)P)←(2mP,(2m+1)P)
409
スカラー倍演算結果出力
413
終了

FIG. 5

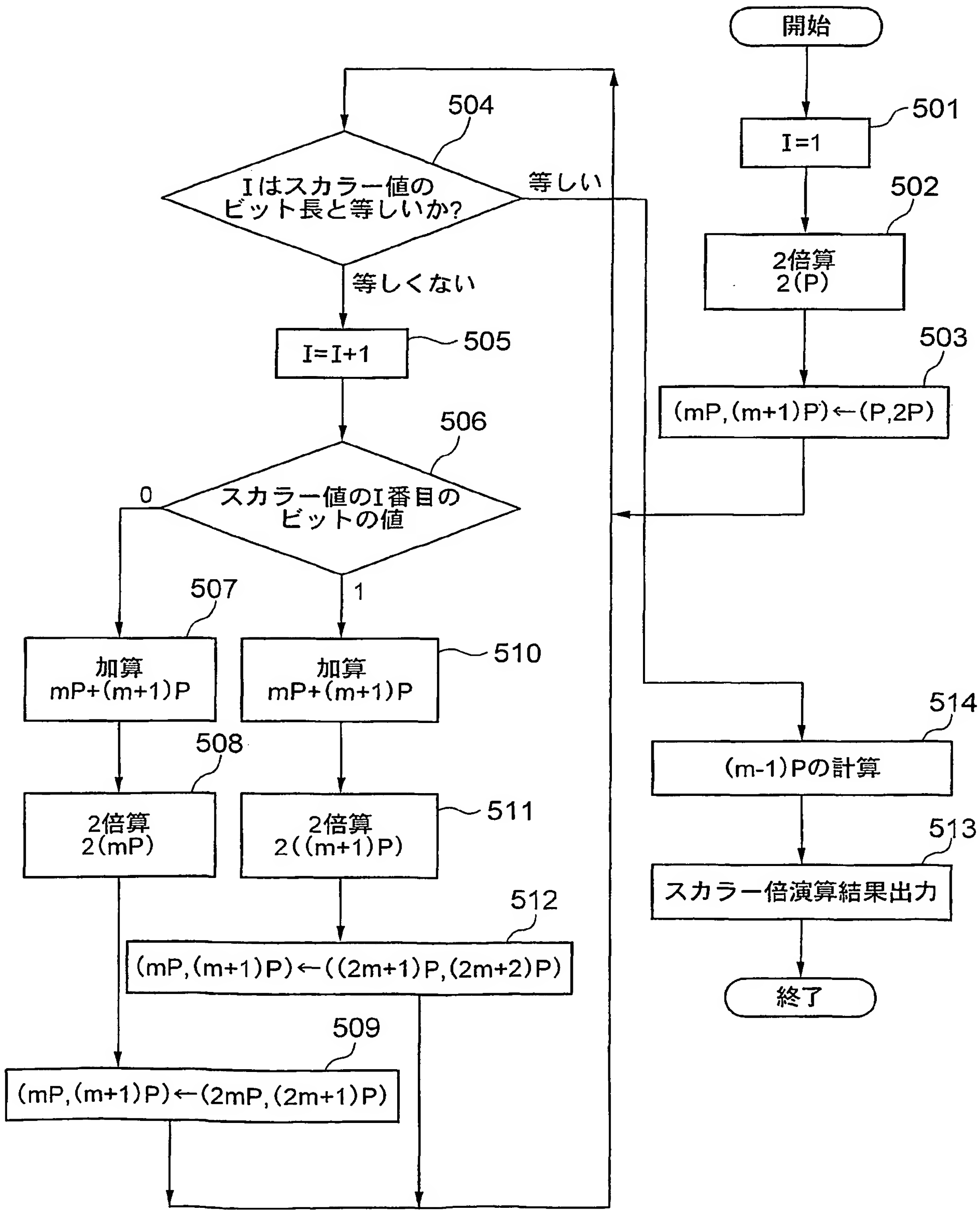

開始
501
I=1
502
2倍算
2(P)
503
(mP,(m+1)P)←(P,2P)
504
Iはスカラー値の
ビット長と等しいか?
等しい
等しくない
505
I=I+1
506
スカラー値のI番目の
ビットの値
0
1
507
加算
mP+(m+1)P
510
加算
mP+(m+1)P
508
2倍算
2(mP)
511
2倍算
2((m+1)P)
512
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
509
(mP,(m+1)P)←(2mP,(2m+1)P)
514
(m-1)Pの計算
513
スカラー倍演算結果出力
終了

FIG. 6

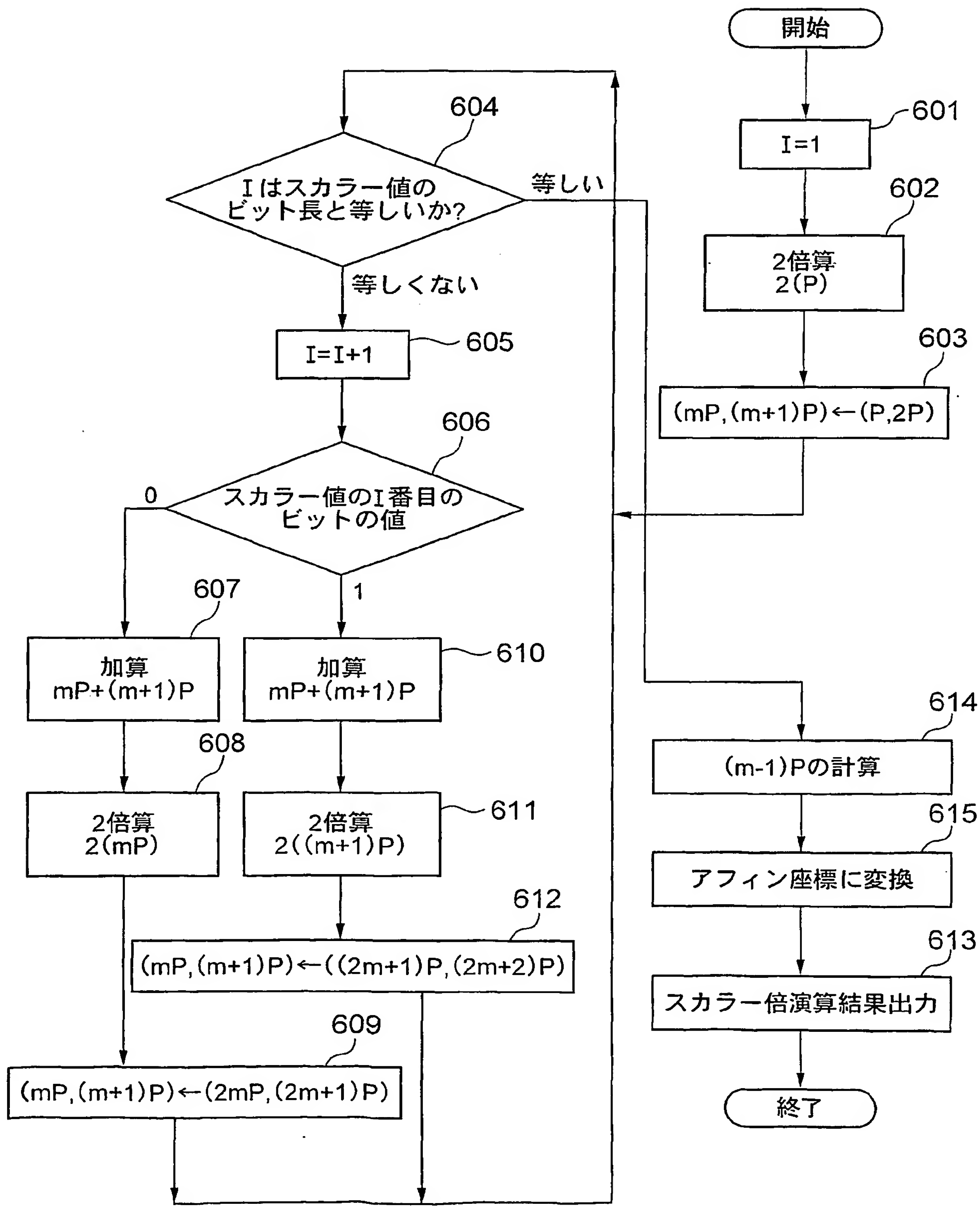
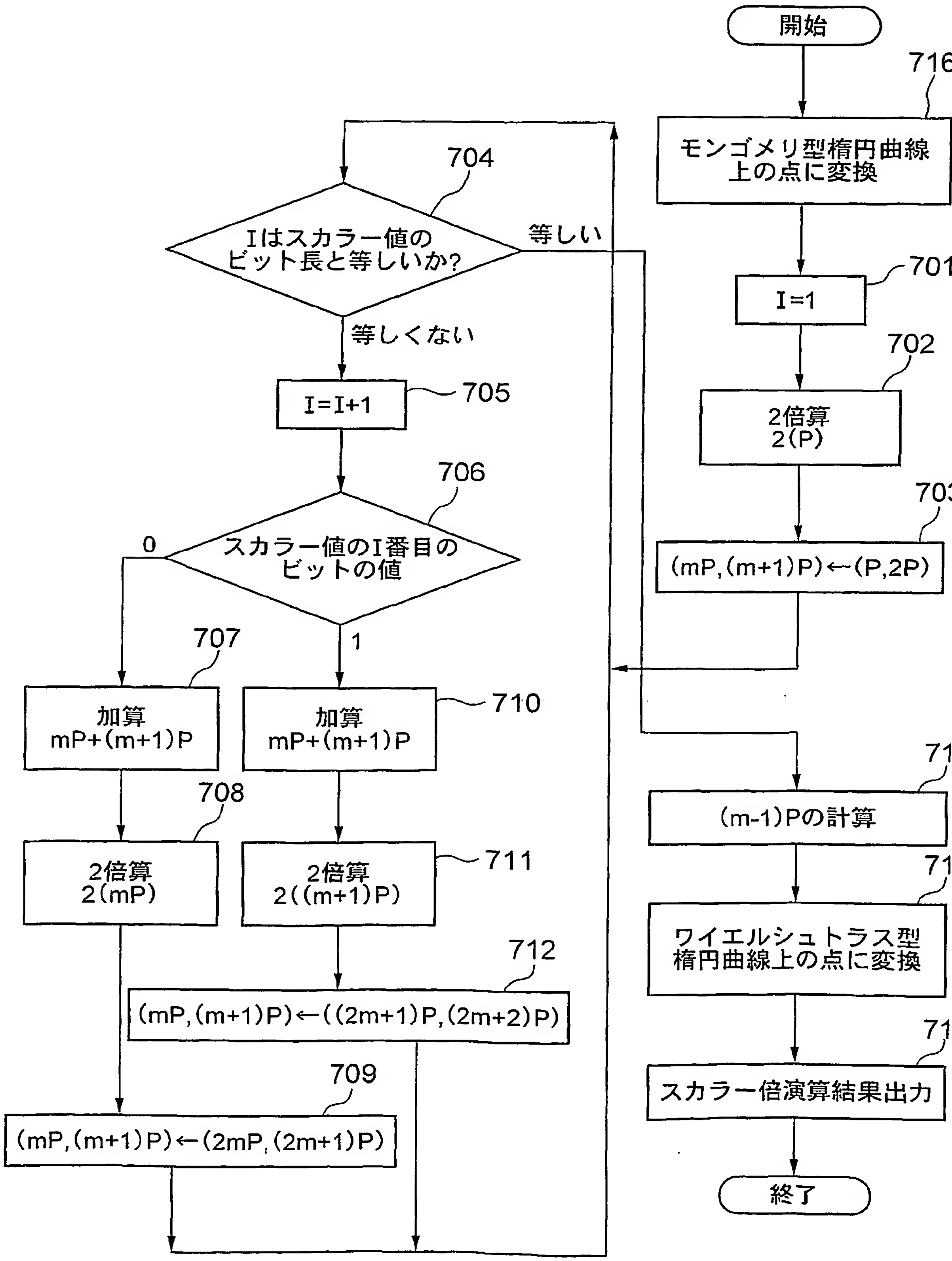

開始
601
I=1
602
2倍算
2(P)
603
(mP,(m+1)P)←(P,2P)
604
Iはスカラー値の
ビット長と等しいか?
等しい
等しくない
605
I=I+1
606
スカラー値のI番目の
ビットの値
0
1
607
加算
mP+(m+1)P
610
加算
mP+(m+1)P
608
2倍算
2(mP)
611
2倍算
2((m+1)P)
612
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
609
(mP,(m+1)P)←(2mP,(2m+1)P)
614
(m-1)Pの計算
615
アフィン座標に変換
613
スカラー倍演算結果出力
終了

FIG. 7



開始
716
モンゴメリ型楕円曲線上の点に変換
701
I=1
702
2倍算
2(P)
703
(mP,(m+1)P)←(P,2P)
704
Iはスカラー値のビット長と等しいか?
等しい
等しくない
705
I=I+1
706
スカラー値のI番目のビットの値
0
1
707
加算
mP+(m+1)P
710
加算
mP+(m+1)P
708
2倍算
2(mP)
711
2倍算
2((m+1)P)
712
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
709
(mP,(m+1)P)←(2mP,(2m+1)P)
714
(m-1)Pの計算
715
ワイエルシュトラス型楕円曲線上の点に変換
713
スカラー倍演算結果出力
終了

FIG. 8

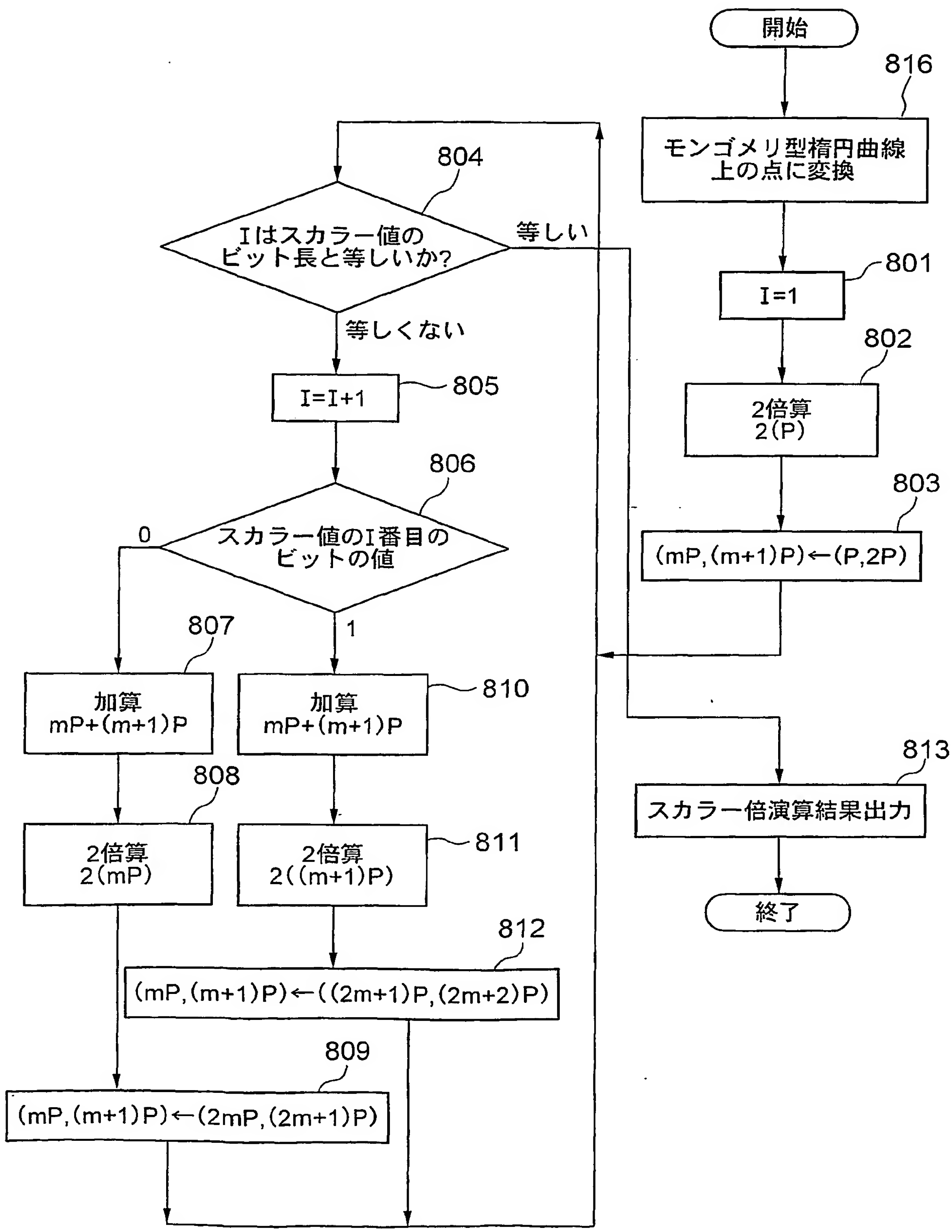

開始
816
モンゴメリ型楕円曲線上の点に変換
801
I=1
802
2倍算
2(P)
803
(mP,(m+1)P)←(P,2P)
804
Iはスカラー値のビット長と等しいか?
等しい
等しくない
805
I=I+1
806
スカラー値のI番目のビットの値
0
1
807
加算
mP+(m+1)P
808
2倍算
2(mP)
809
(mP,(m+1)P)←(2mP,(2m+1)P)
810
加算
mP+(m+1)P
811
2倍算
2((m+1)P)
812
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
813
スカラー倍演算結果出力
終了

FIG. 9

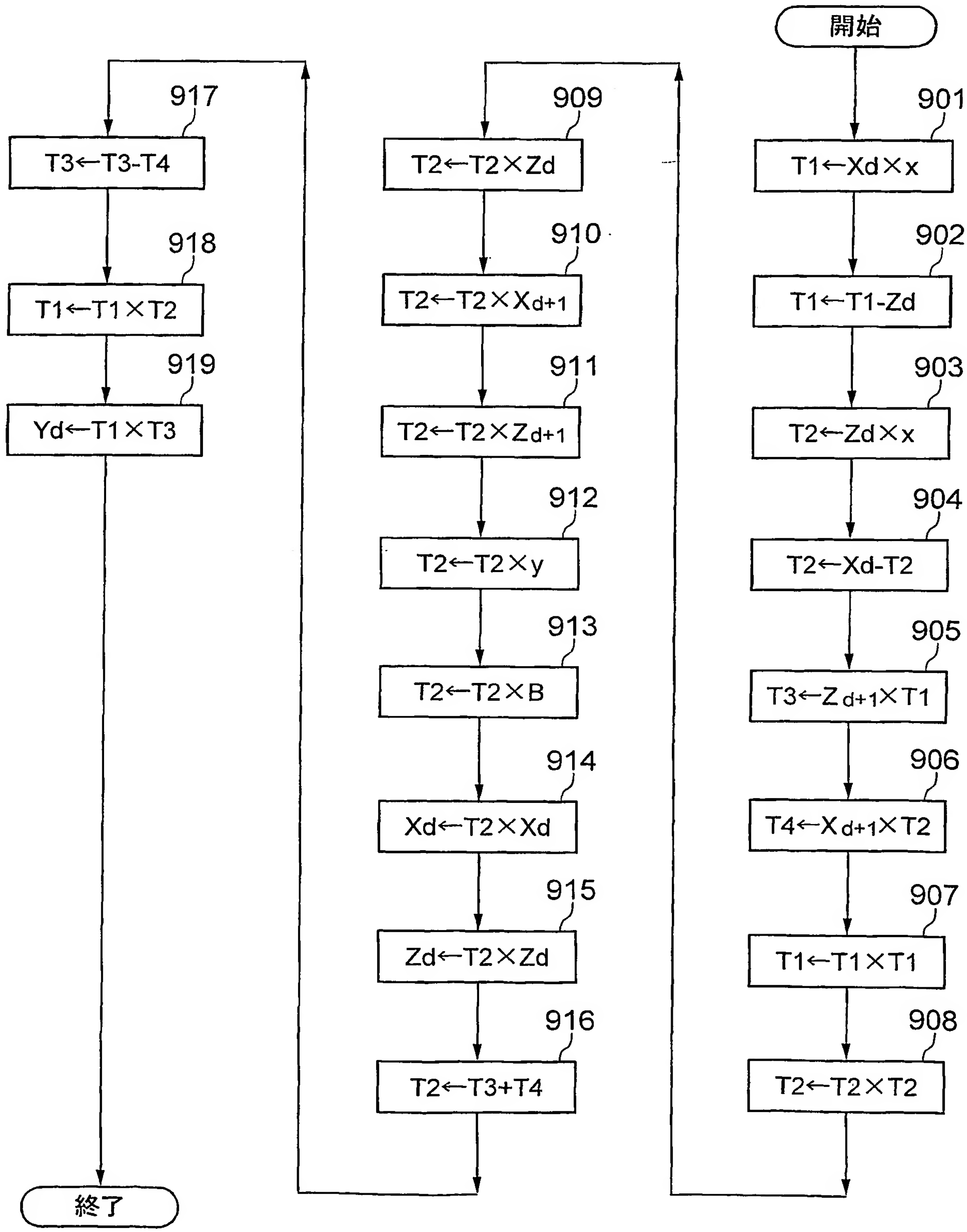

開始
901
T1←Xd×x
902
T1←T1-Zd
903
T2←Zd×x
904
T2←Xd-T2
905
T3←Zd+1×T1
906
T4←Xd+1×T2
907
T1←T1×T1
908
T2←T2×T2
909
T2←T2×Zd
910
T2←T2×Xd+1
911
T2←T2×Zd+1
912
T2←T2×y
913
T2←T2×B
914
Xd←T2×Xd
915
Zd←T2×Zd
916
T2←T3+T4
917
T3←T3-T4
918
T1←T1×T2
919
Yd←T1×T3
終了

FIG. 10

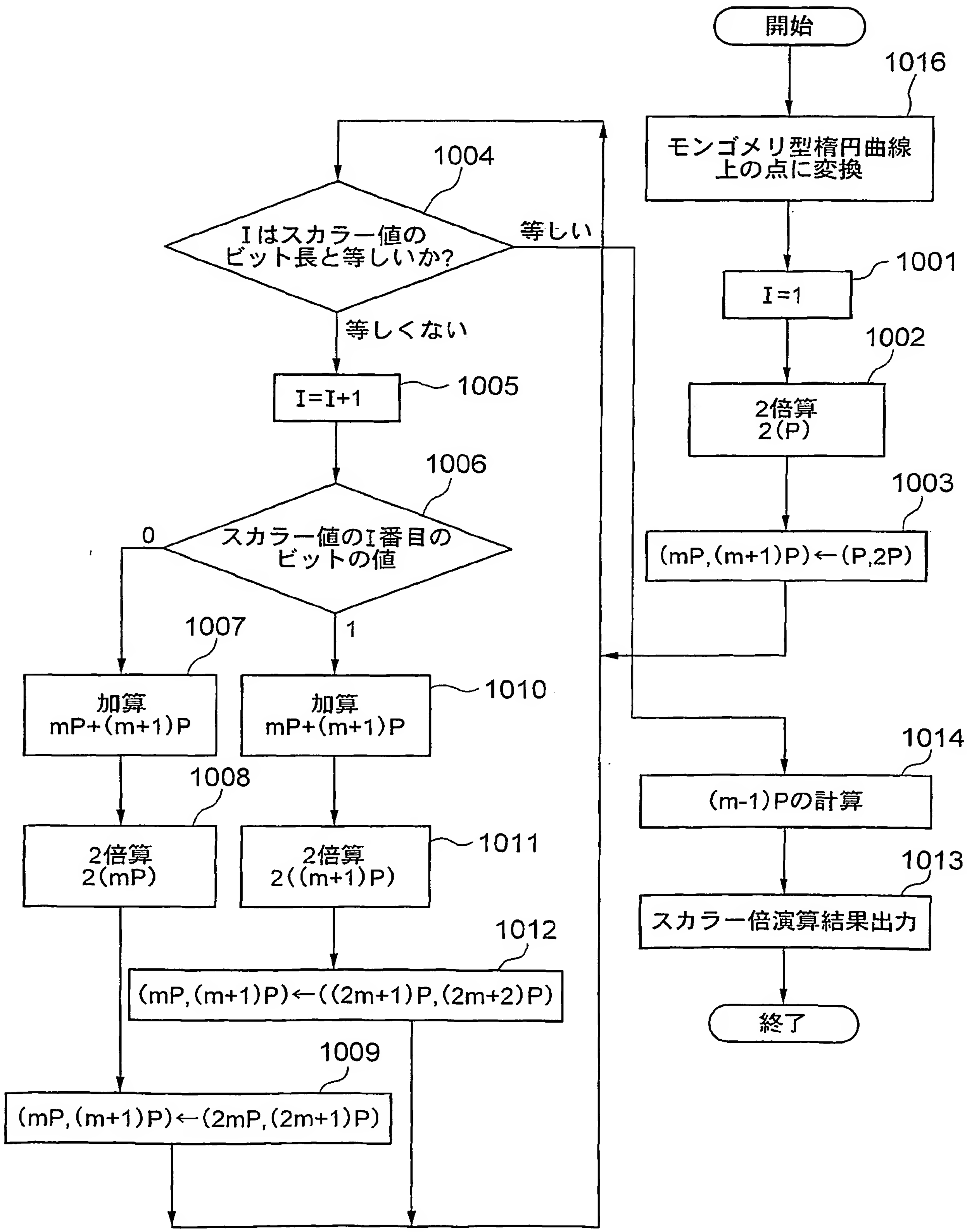

開始
1016
モンゴメリ型楕円曲線
上の点に変換
1001
I=1
1002
2倍算
2(P)
1003
(mP,(m+1)P)←(P,2P)
1004
Iはスカラー値の
ビット長と等しいか?
等しい
等しくない
1005
I=I+1
1006
スカラー値のI番目の
ビットの値
0
1
1007
加算
mP+(m+1)P
1010
加算
mP+(m+1)P
1008
2倍算
2(mP)
1011
2倍算
2((m+1)P)
1012
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
1009
(mP,(m+1)P)←(2mP,(2m+1)P)
1014
(m-1)Pの計算
1013
スカラー倍演算結果出力
終了

FIG. 11

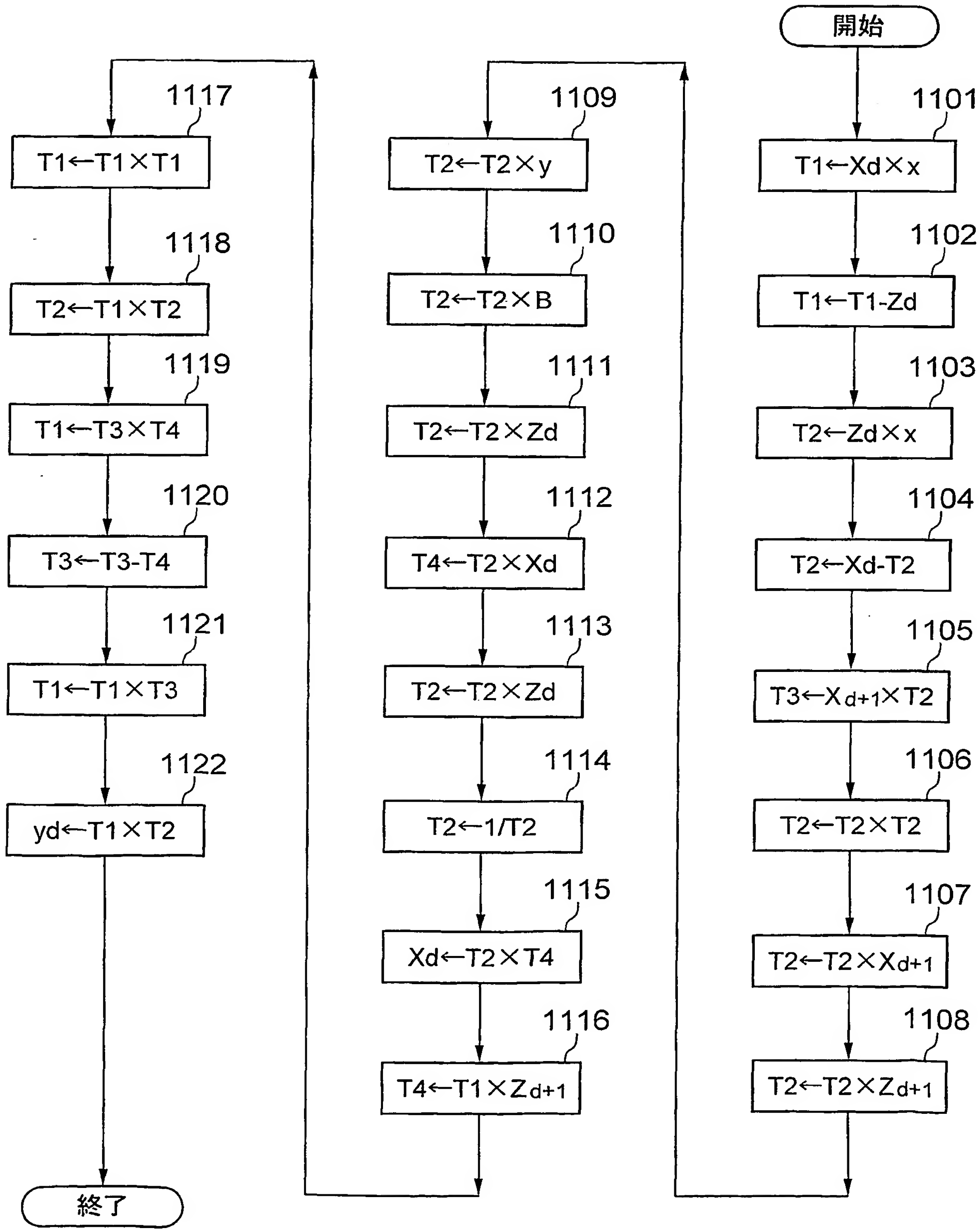

開始
1101
T1←Xd×x
1102
T1←T1-Zd
1103
T2←Zd×x
1104
T2←Xd-T2
1105
T3←Xd+1×T2
1106
T2←T2×T2
1107
T2←T2×Xd+1
1108
T2←T2×Zd+1
1109
T2←T2×y
1110
T2←T2×B
1111
T2←T2×Zd
1112
T4←T2×Xd
1113
T2←T2×Zd
1114
T2←1/T2
1115
Xd←T2×T4
1116
T4←T1×Zd+1
1117
T1←T1×T1
1118
T2←T1×T2
1119
T1←T3×T4
1120
T3←T3-T4
1121
T1←T1×T3
1122
yd←T1×T2
終了

FIG. 12

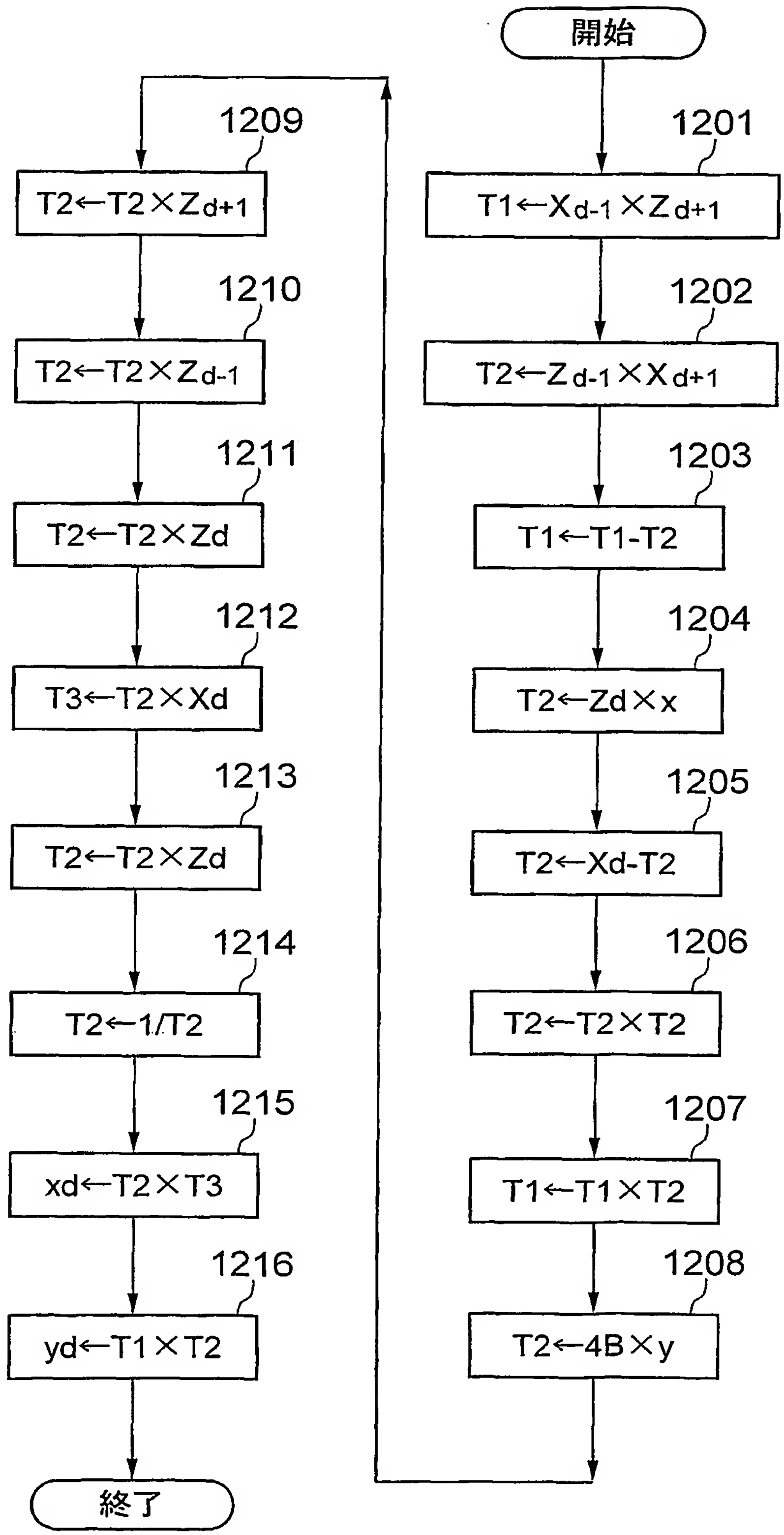
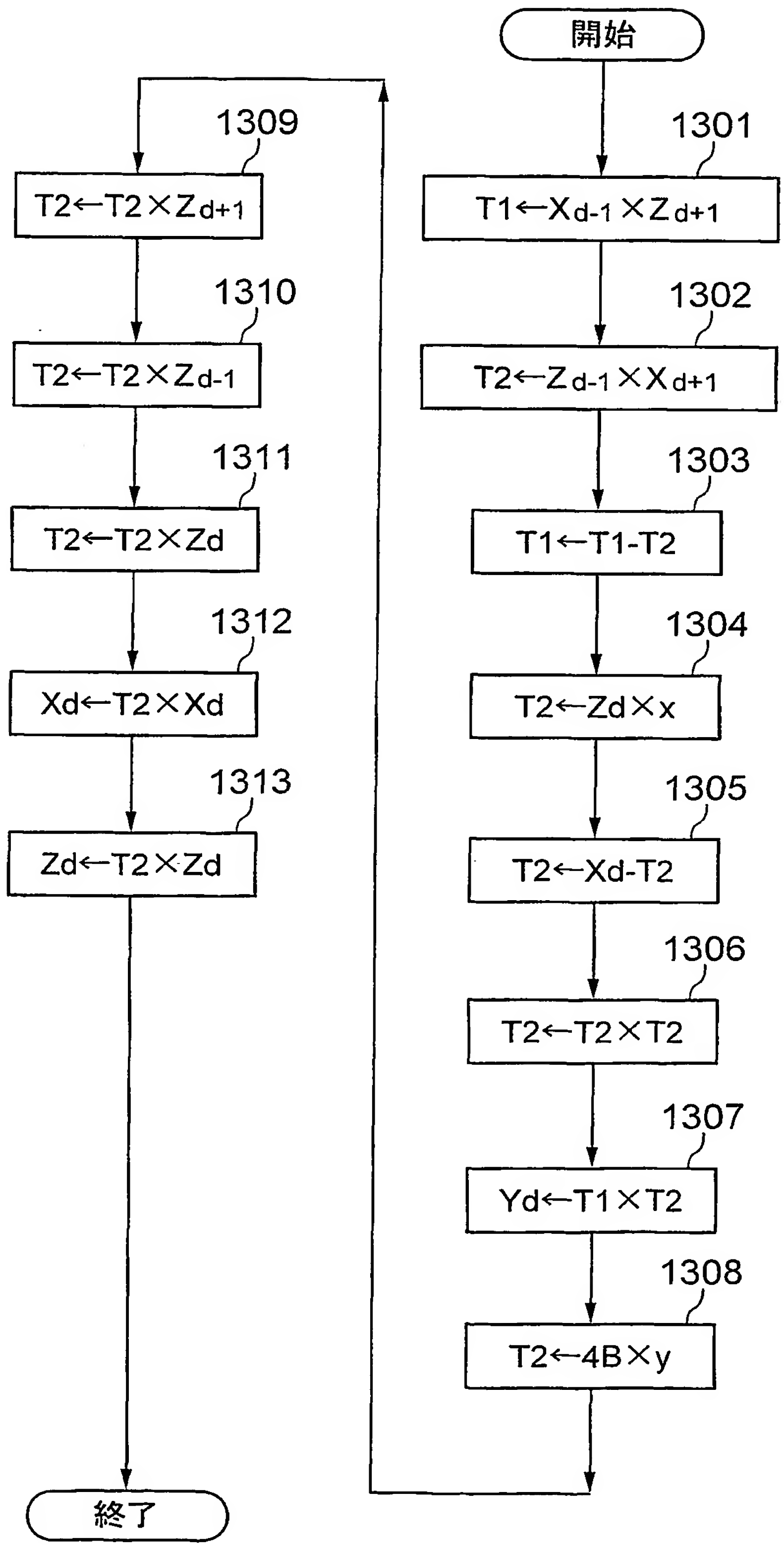
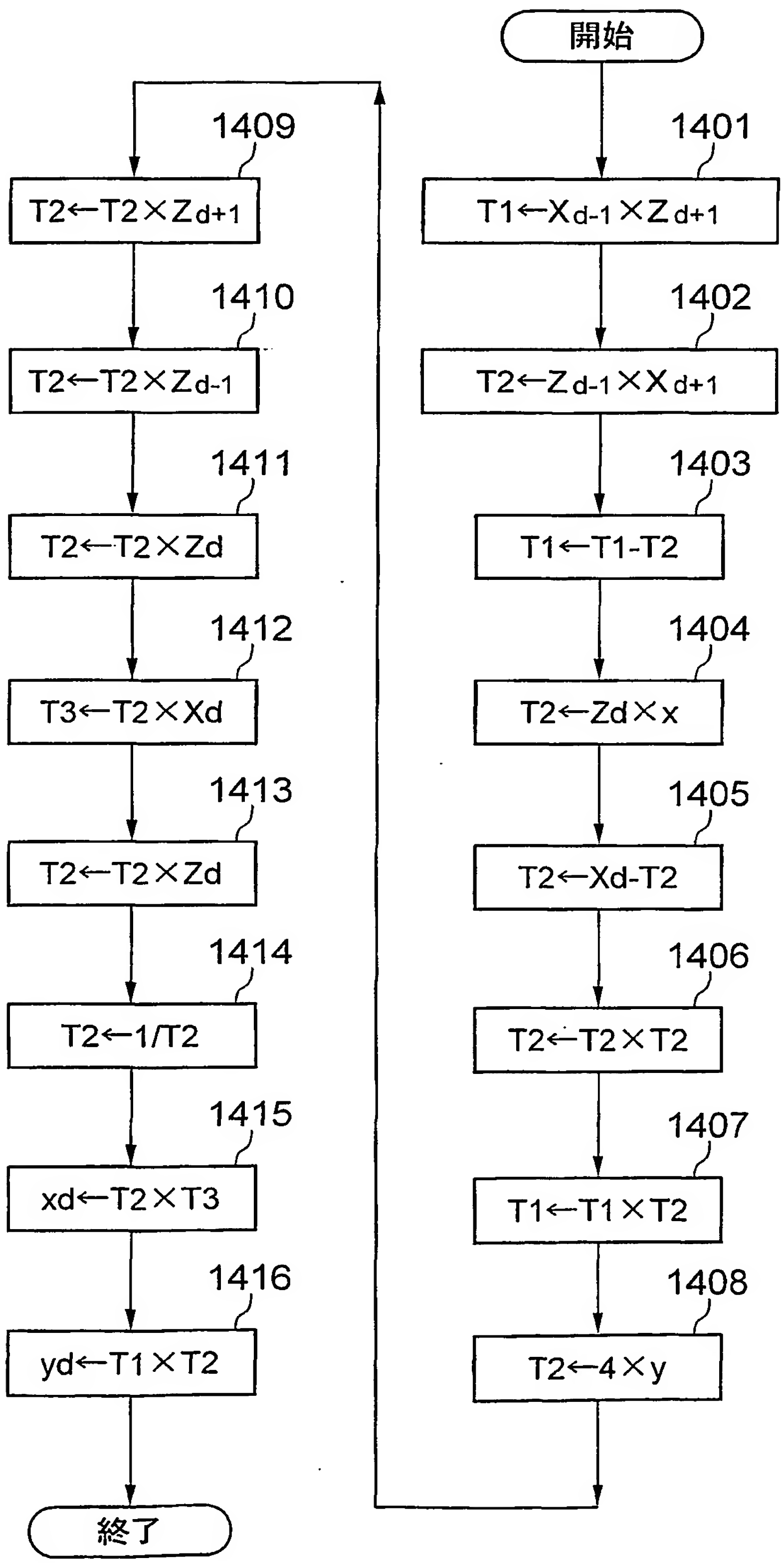

開始
1201
T1←Xd-1×Zd+1
1202
T2←Zd-1×Xd+1
1203
T1←T1-T2
1204
T2←Zd×x
1205
T2←Xd-T2
1206
T2←T2×T2
1207
T1←T1×T2
1208
T2←4B×y
1209
T2←T2×Zd+1
1210
T2←T2×Zd-1
1211
T2←T2×Zd
1212
T3←T2×Xd
1213
T2←T2×Zd
1214
T2←1/T2
1215
xd←T2×T3
1216
yd←T1×T2
終了

FIG. 13


開始
1301
T1←Xd-1×Zd+1
1302
T2←Zd-1×Xd+1
1303
T1←T1-T2
1304
T2←Zd×x
1305
T2←Xd-T2
1306
T2←T2×T2
1307
Yd←T1×T2
1308
T2←4B×y
1309
T2←T2×Zd+1
1310
T2←T2×Zd-1
1311
T2←T2×Zd
1312
Xd←T2×Xd
1313
Zd←T2×Zd
終了

# FIG. 14


開始
1401
T1←Xd-1×Zd+1
1402
T2←Zd-1×Xd+1
1403
T1←T1-T2
1404
T2←Zd×x
1405
T2←Xd-T2
1406
T2←T2×T2
1407
T1←T1×T2
1408
T2←4×y
1409
T2←T2×Zd+1
1410
T2←T2×Zd-1
1411
T2←T2×Zd
1412
T3←T2×Xd
1413
T2←T2×Zd
1414
T2←1/T2
1415
xd←T2×T3
1416
yd←T1×T2
終了

# FIG. 15

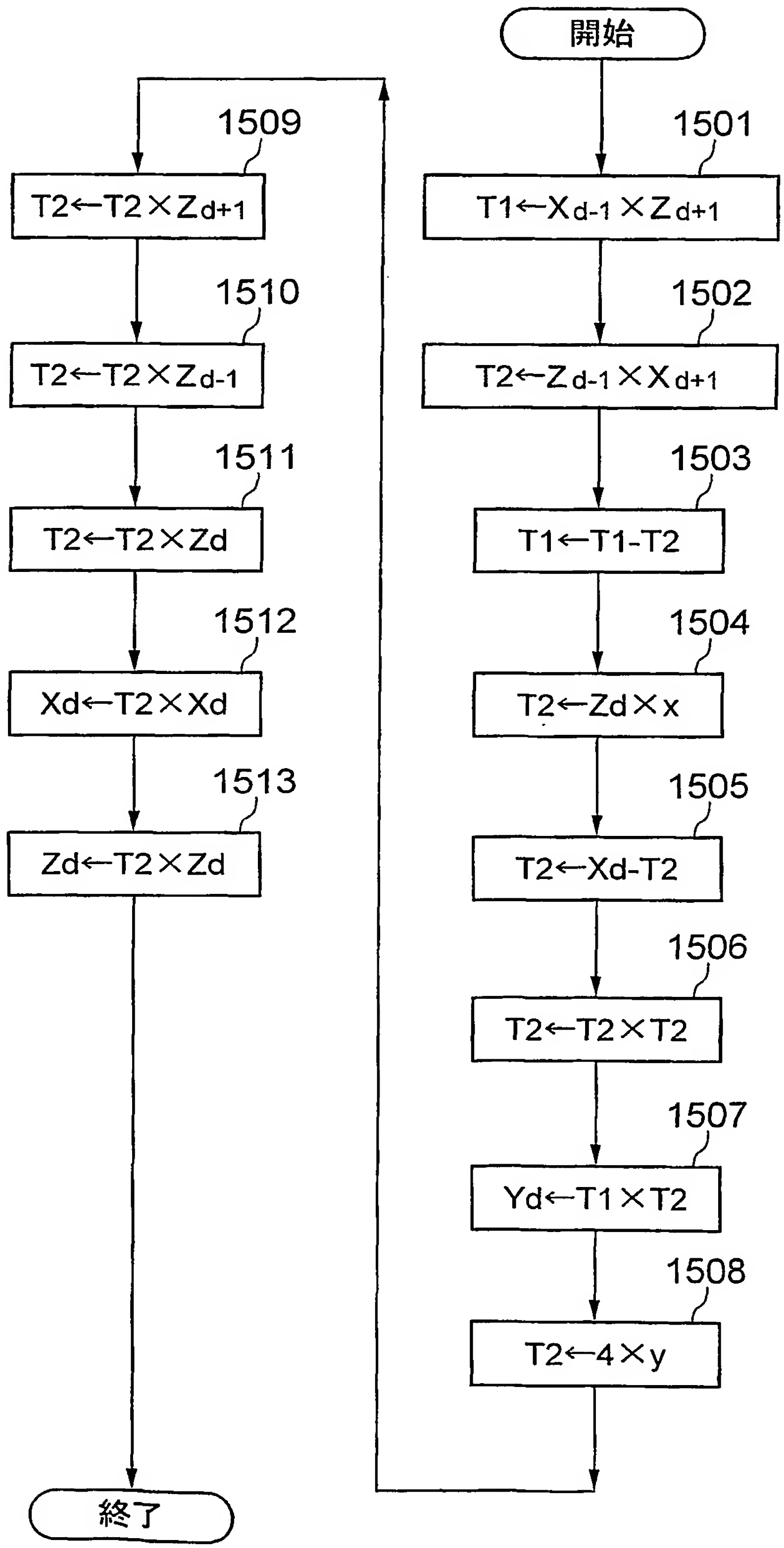

開始
1501
T1←Xd-1×Zd+1
1502
T2←Zd-1×Xd+1
1503
T1←T1-T2
1504
T2←Zd×x
1505
T2←Xd-T2
1506
T2←T2×T2
1507
Yd←T1×T2
1508
T2←4×y
1509
T2←T2×Zd+1
1510
T2←T2×Zd-1
1511
T2←T2×Zd
1512
Xd←T2×Xd
1513
Zd←T2×Zd
終了

FIG. 16

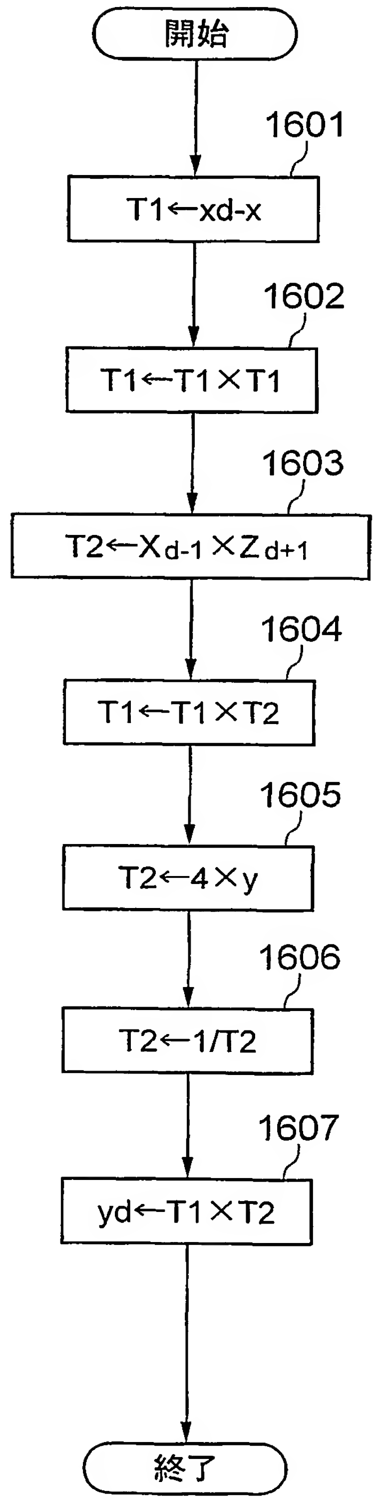

開始
1601
T1←xd-x
1602
T1←T1×T1
1603
T2←Xd-1×Zd+1
1604
T1←T1×T2
1605
T2←4×y
1606
T2←1/T2
1607
yd←T1×T2
終了

FIG. 17

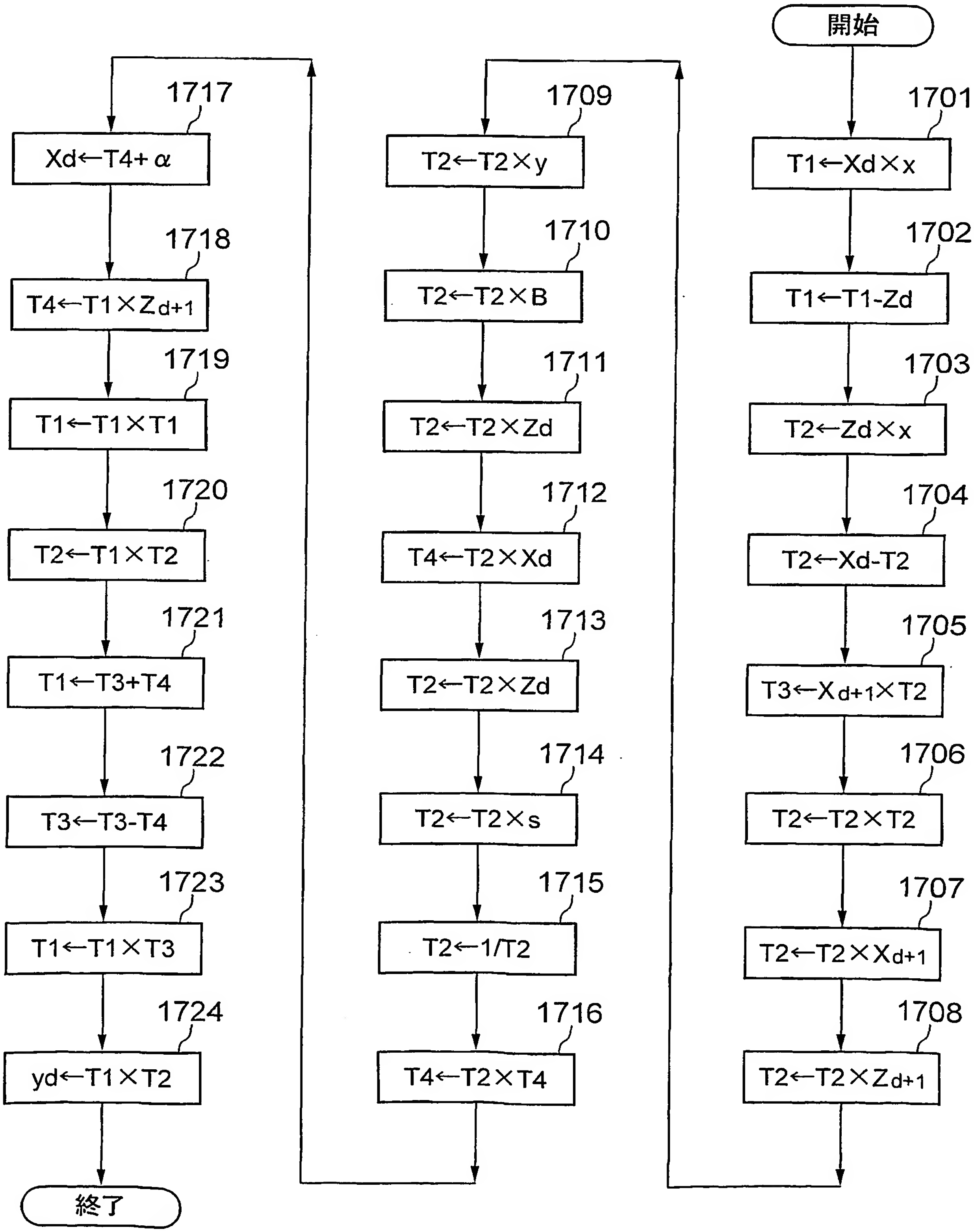

開始
1701
T1←Xd×x
1702
T1←T1-Zd
1703
T2←Zd×x
1704
T2←Xd-T2
1705
T3←Xd+1×T2
1706
T2←T2×T2
1707
T2←T2×Xd+1
1708
T2←T2×Zd+1
1709
T2←T2×y
1710
T2←T2×B
1711
T2←T2×Zd
1712
T4←T2×Xd
1713
T2←T2×Zd
1714
T2←T2×s
1715
T2←1/T2
1716
T4←T2×T4
1717
Xd←T4+α
1718
T4←T1×Zd+1
1719
T1←T1×T1
1720
T2←T1×T2
1721
T1←T3+T4
1722
T3←T3-T4
1723
T1←T1×T3
1724
yd←T1×T2
終了

FIG. 18

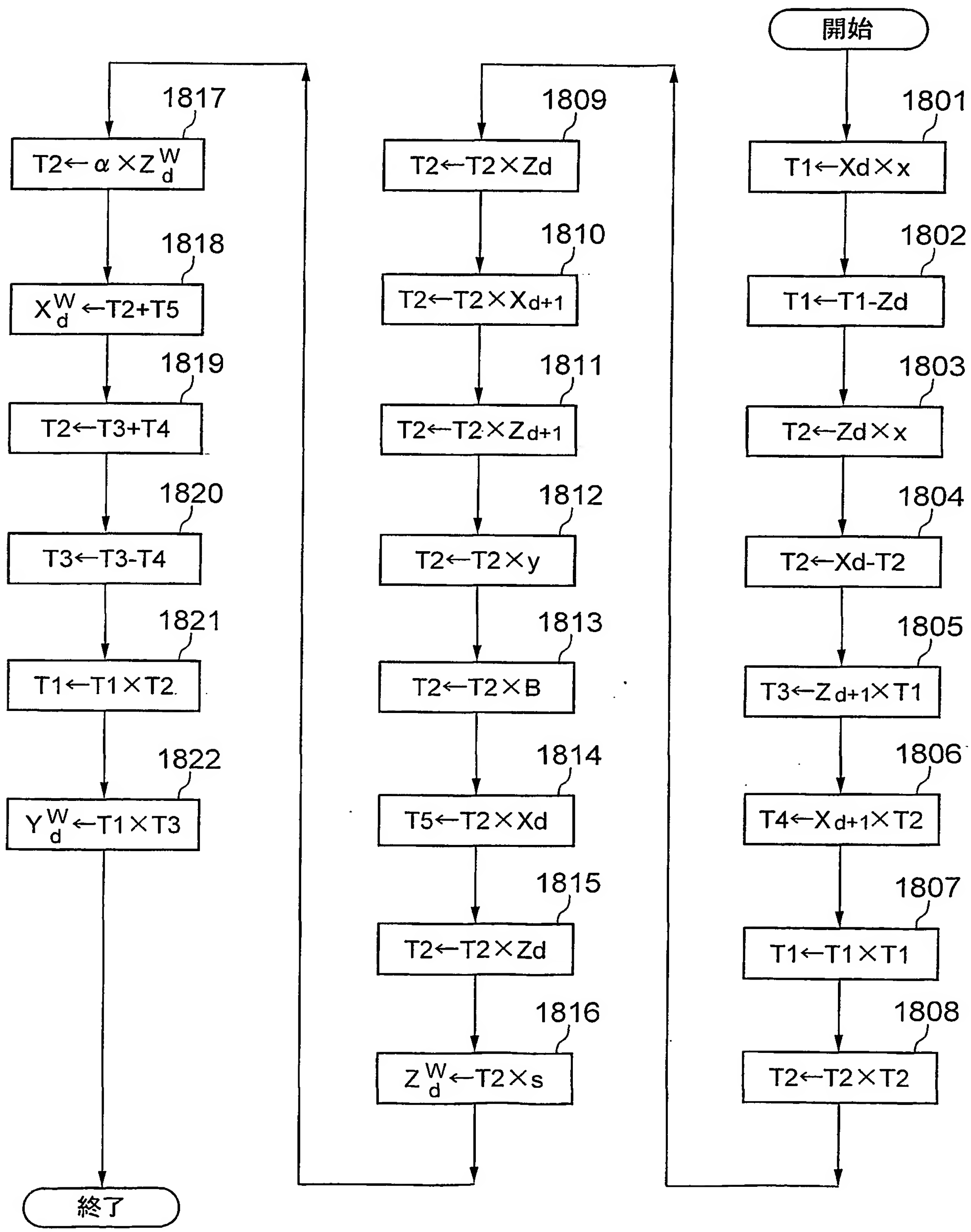

開始
1801
T1←Xd×x
1802
T1←T1-Zd
1803
T2←Zd×x
1804
T2←Xd-T2
1805
T3←Zd+1×T1
1806
T4←Xd+1×T2
1807
T1←T1×T1
1808
T2←T2×T2
1809
T2←T2×Zd
1810
T2←T2×Xd+1
1811
T2←T2×Zd+1
1812
T2←T2×y
1813
T2←T2×B
1814
T5←T2×Xd
1815
T2←T2×Zd
1816
Z W d←T2×s
1817
T2←α×Z W d
1818
X W d←T2+T5
1819
T2←T3+T4
1820
T3←T3-T4
1821
T1←T1×T2
1822
Y W d←T1×T3
終了

FIG. 19

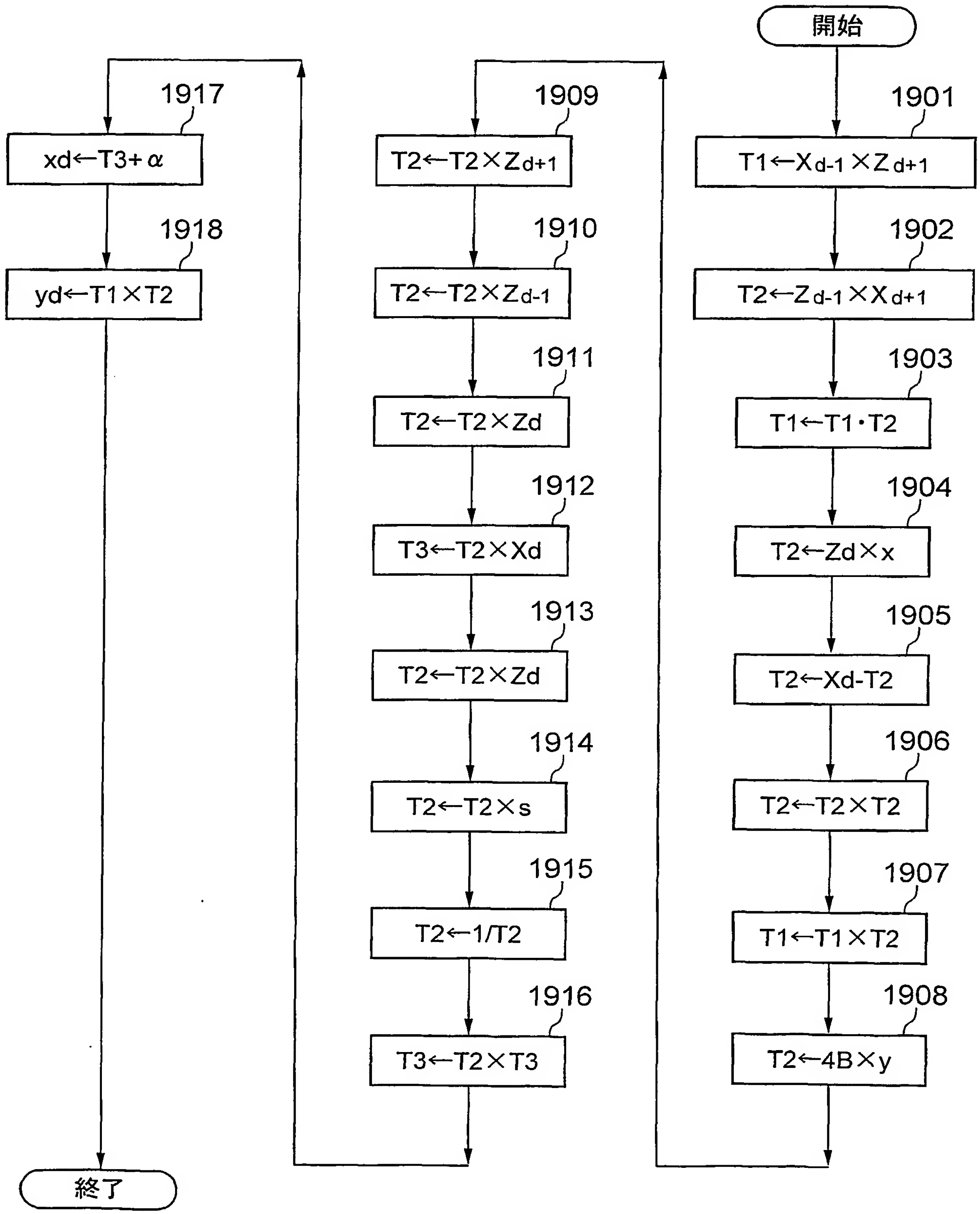

開始
1901
T1←Xd-1×Zd+1
1902
T2←Zd-1×Xd+1
1903
T1←T1·T2
1904
T2←Zd×x
1905
T2←Xd-T2
1906
T2←T2×T2
1907
T1←T1×T2
1908
T2←4B×y
1909
T2←T2×Zd+1
1910
T2←T2×Zd-1
1911
T2←T2×Zd
1912
T3←T2×Xd
1913
T2←T2×Zd
1914
T2←T2×s
1915
T2←1/T2
1916
T3←T2×T3
1917
xd←T3+α
1918
yd←T1×T2
終了

FIG. 20

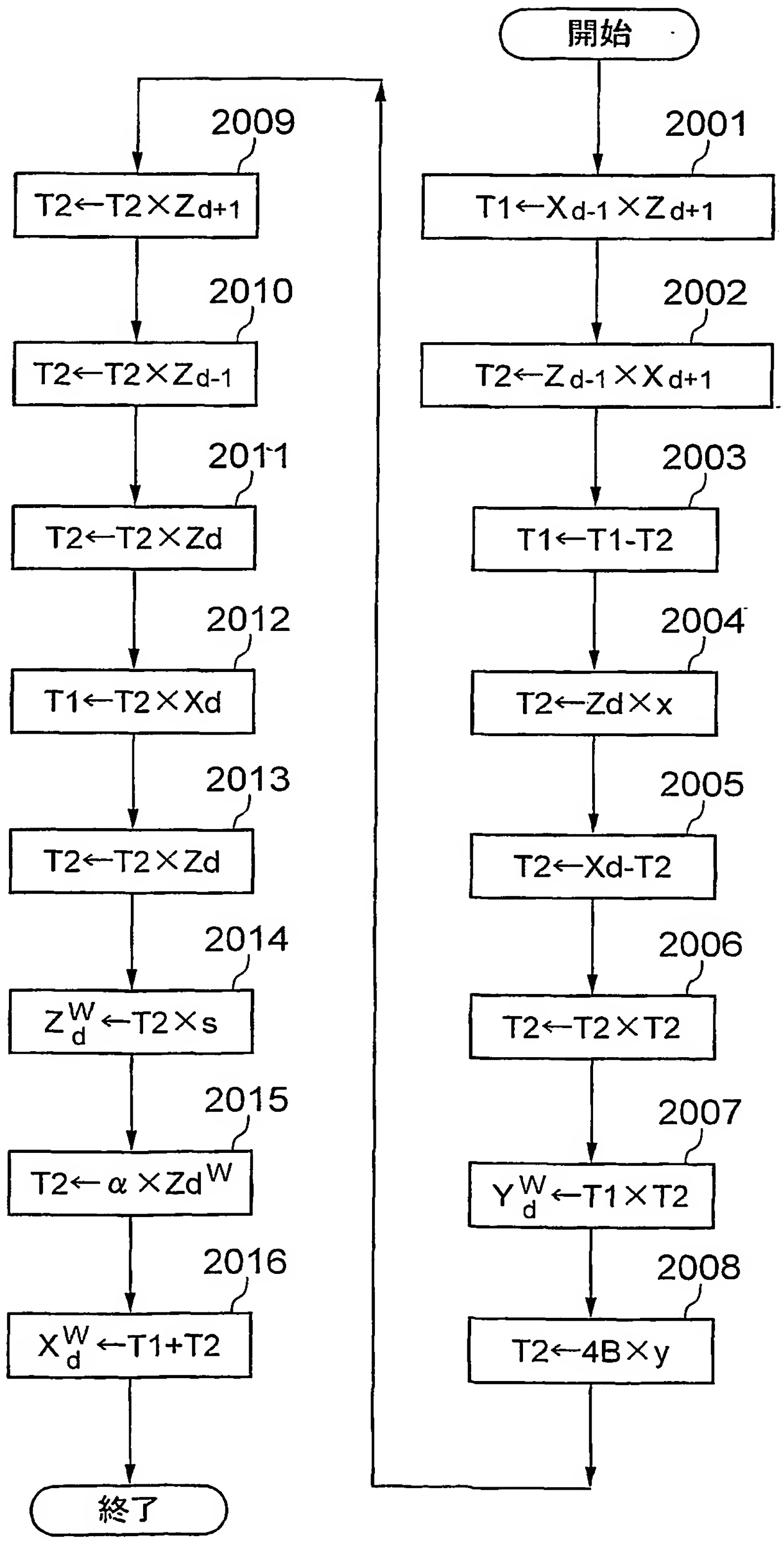

開始
2001
T1←Xd-1×Zd+1
2002
T2←Zd-1×Xd+1
2003
T1←T1-T2
2004
T2←Zd×x
2005
T2←Xd-T2
2006
T2←T2×T2
2007
Y W d ←T1×T2
2008
T2←4B×y
2009
T2←T2×Zd+1
2010
T2←T2×Zd-1
2011
T2←T2×Zd
2012
T1←T2×Xd
2013
T2←T2×Zd
2014
Z W d ←T2×s
2015
T2←α×Zd W
2016
X W d ←T1+T2
終了

FIG. 21

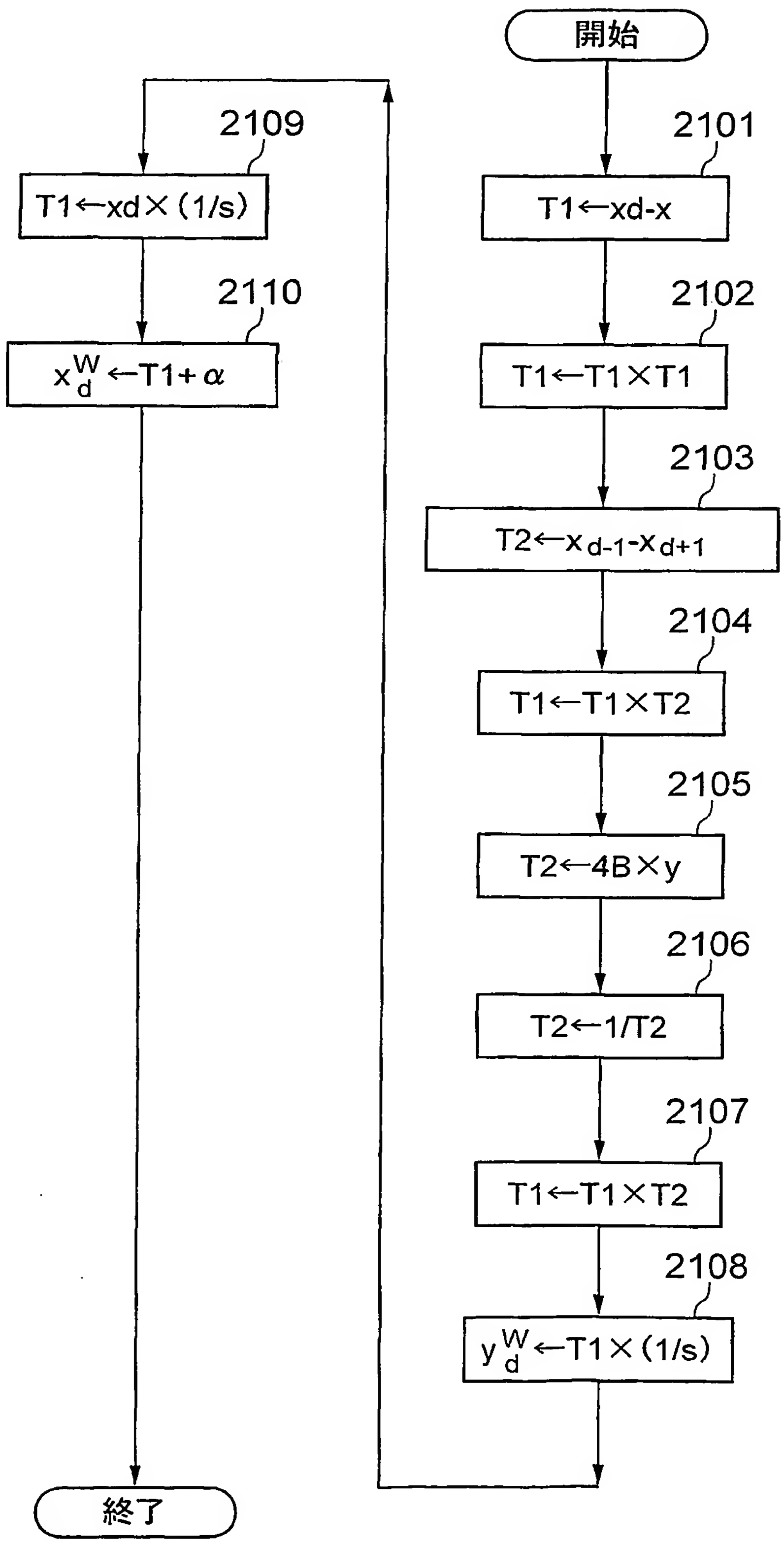

開始
2101
T1←xd-x
2102
T1←T1×T1
2103
T2←x d-1-x d+1
2104
T1←T1×T2
2105
T2←4B×y
2106
T2←1/T2
2107
T1←T1×T2
2108
$y_d^W$←T1×(1/s)
2109
T1←xd×(1/s)
2110
$x_d^W$←T1+α
終了

FIG. 22

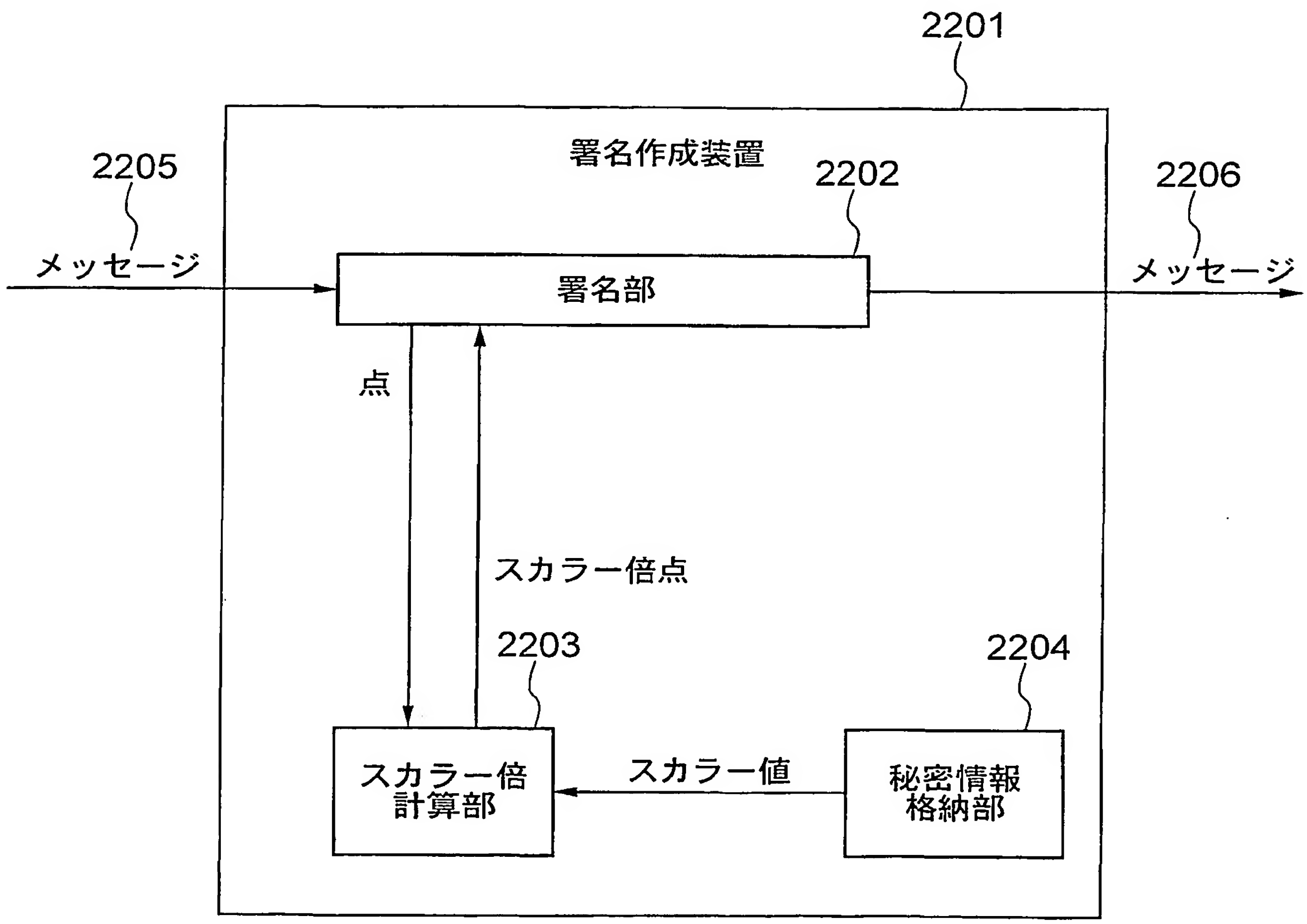

2201
署名作成装置
2205
メッセージ
2202
署名部
2206
メッセージ
点
スカラー倍点
2203
2204
スカラー倍計算部
スカラー値
秘密情報格納部

FIG. 23

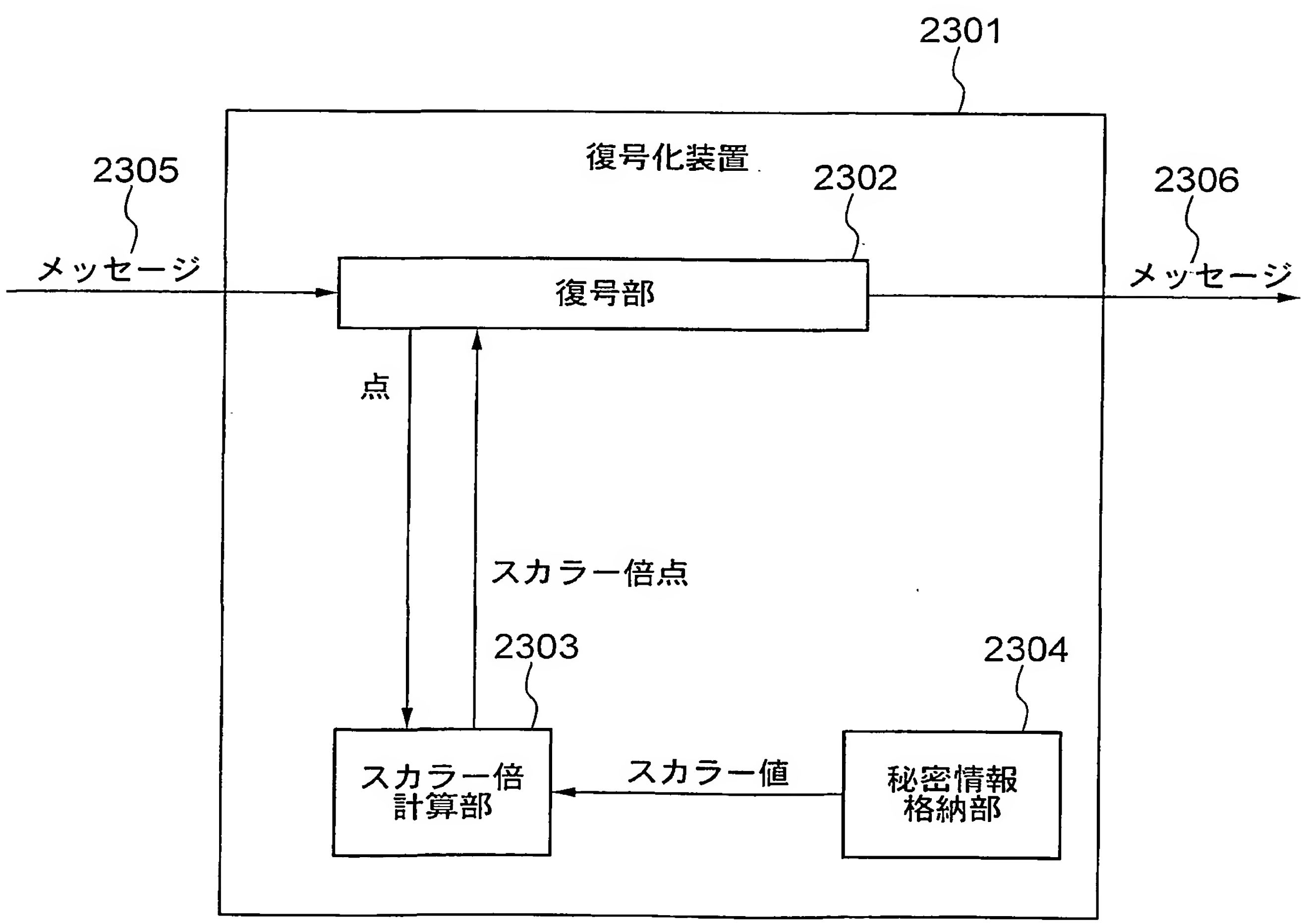
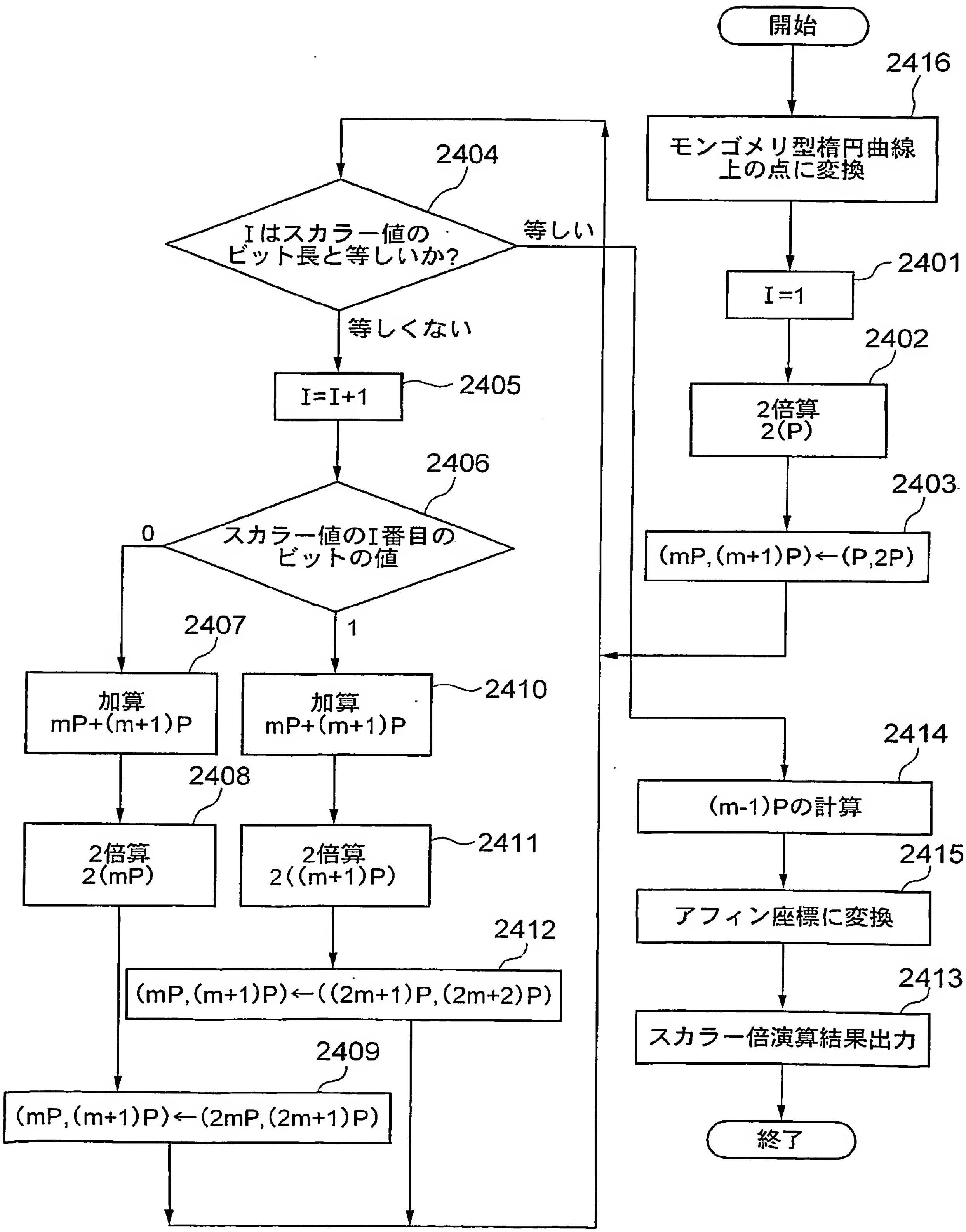

2301
復号化装置
2302
2305
メッセージ
復号部
2306
メッセージ
点
スカラー倍点
2303
2304
スカラー倍
計算部
スカラー値
秘密情報
格納部

FIG. 24



開始
2416
モンゴメリ型楕円曲線上の点に変換
2401
I=1
2402
2倍算
2(P)
2403
(mP,(m+1)P)←(P,2P)
2404
Iはスカラー値のビット長と等しいか?
等しい
等しくない
2405
I=I+1
2406
スカラー値のI番目のビットの値
0
1
2407
加算
mP+(m+1)P
2410
加算
mP+(m+1)P
2408
2倍算
2(mP)
2411
2倍算
2((m+1)P)
2412
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
2409
(mP,(m+1)P)←(2mP,(2m+1)P)
2414
(m-1)Pの計算
2415
アフィン座標に変換
2413
スカラー倍演算結果出力
終了

FIG. 25

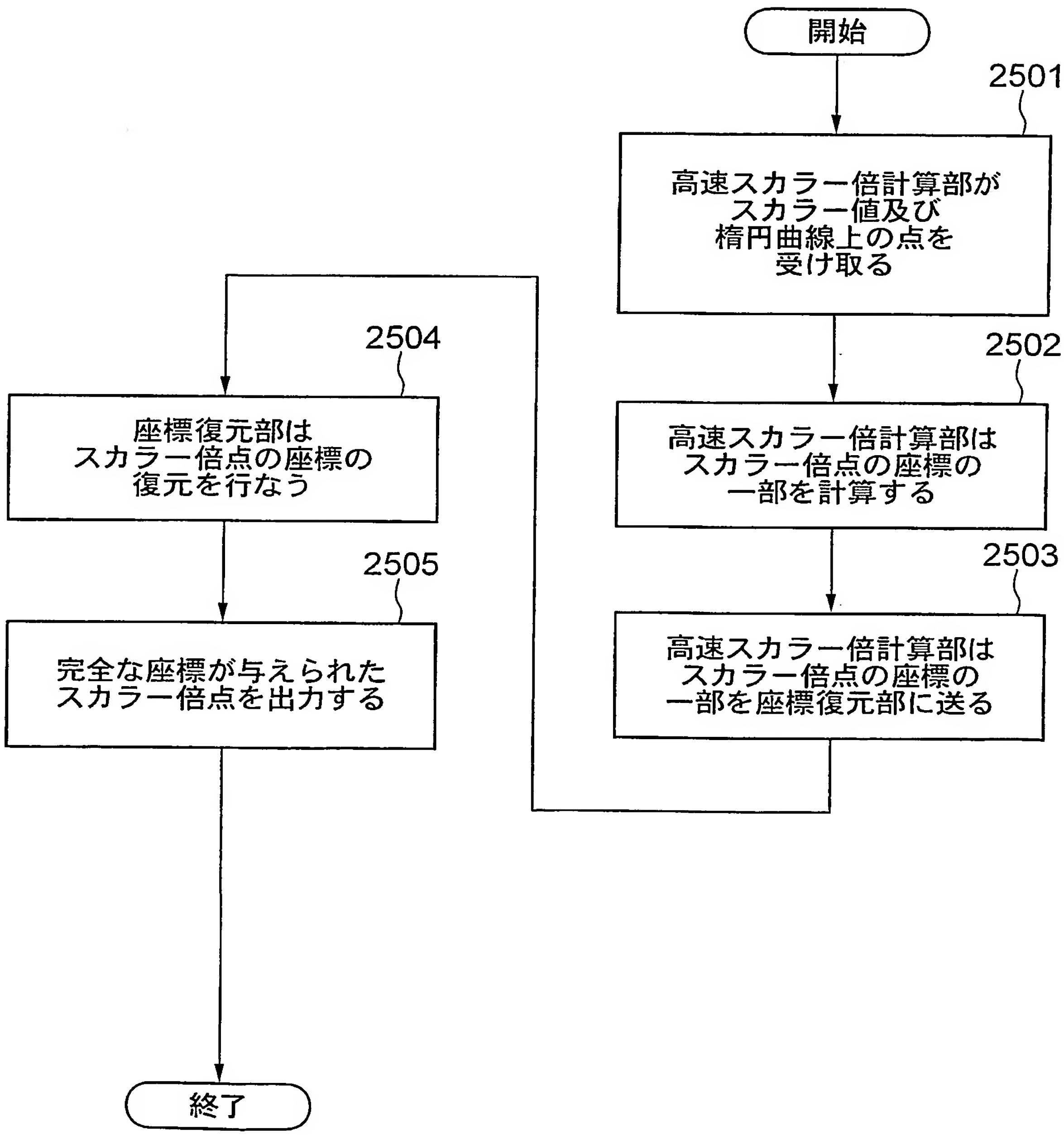

開始
2501
高速スカラー倍計算部がスカラー値及び楕円曲線上の点を受け取る
2502
高速スカラー倍計算部はスカラー倍点の座標の一部を計算する
2503
高速スカラー倍計算部はスカラー倍点の座標の一部を座標復元部に送る
2504
座標復元部はスカラー倍点の座標の復元を行なう
2505
完全な座標が与えられたスカラー倍点を出力する
終了

FIG. 26

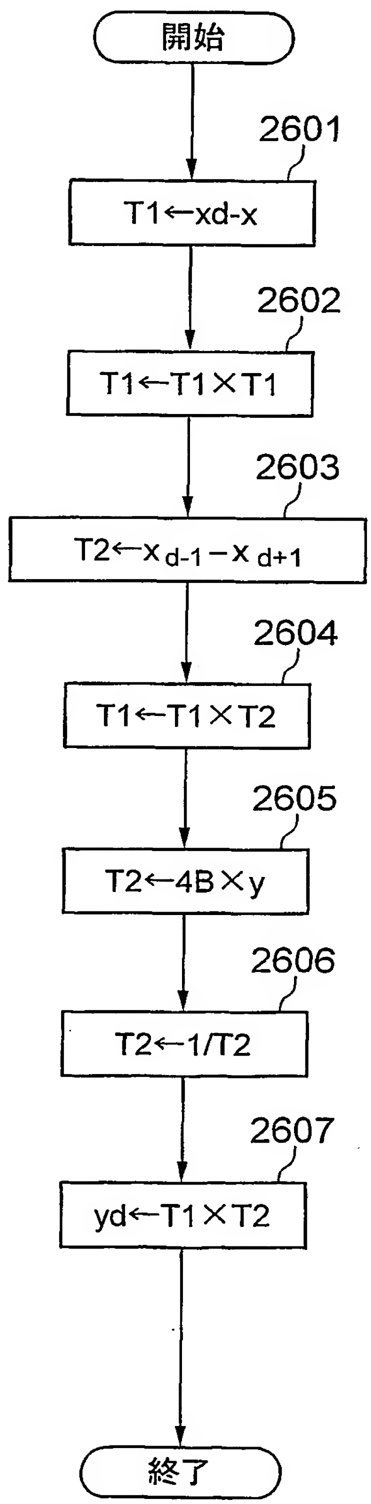

開始
2601
T1←xd-x
2602
T1←T1×T1
2603
T2←x d-1 − x d+1
2604
T1←T1×T2
2605
T2←4B×y
2606
T2←1/T2
2607
yd←T1×T2
終了

FIG. 27

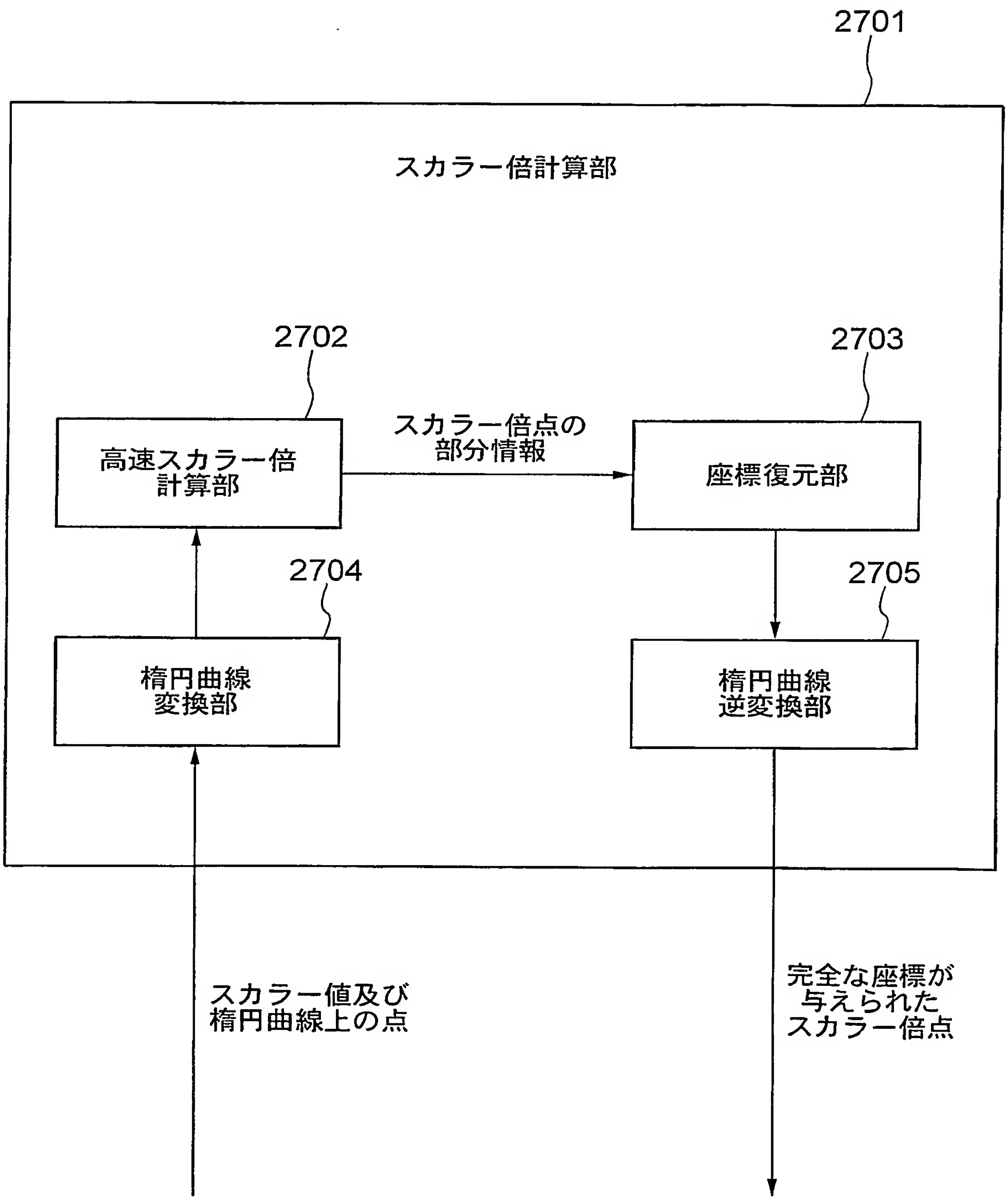

2701
スカラー倍計算部
2702
高速スカラー倍計算部
スカラー倍点の部分情報
2703
座標復元部
2704
楕円曲線変換部
2705
楕円曲線逆変換部
スカラー値及び楕円曲線上の点
完全な座標が与えられたスカラー倍点

FIG. 28

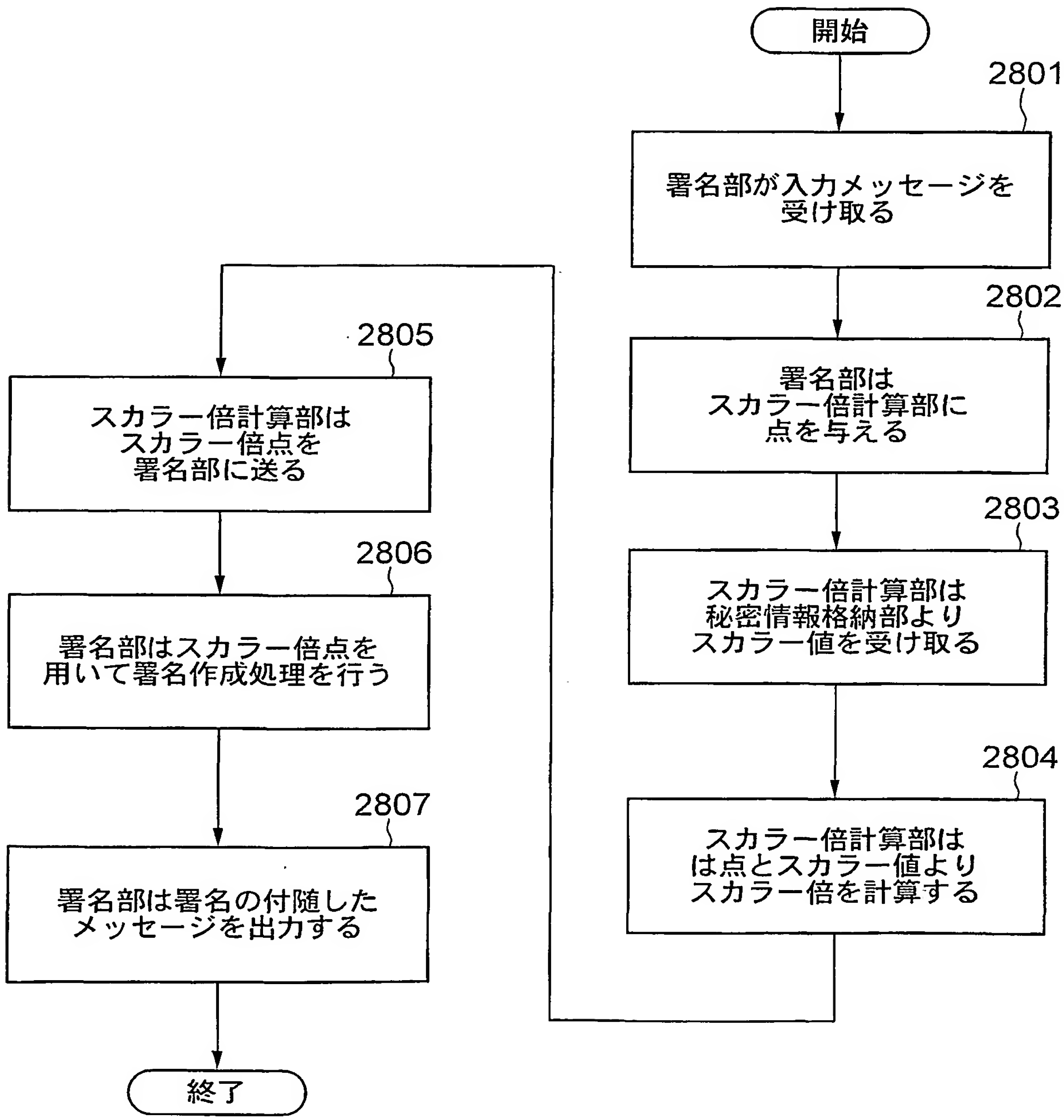

開始
2801
署名部が入力メッセージを受け取る
2802
署名部はスカラー倍計算部に点を与える
2803
スカラー倍計算部は秘密情報格納部よりスカラー値を受け取る
2804
スカラー倍計算部ははは点とスカラー値よりスカラー倍を計算する
2805
スカラー倍計算部はスカラー倍点を署名部に送る
2806
署名部はスカラー倍点を用いて署名作成処理を行う
2807
署名部は署名の付随したメッセージを出力する
終了

FIG. 29

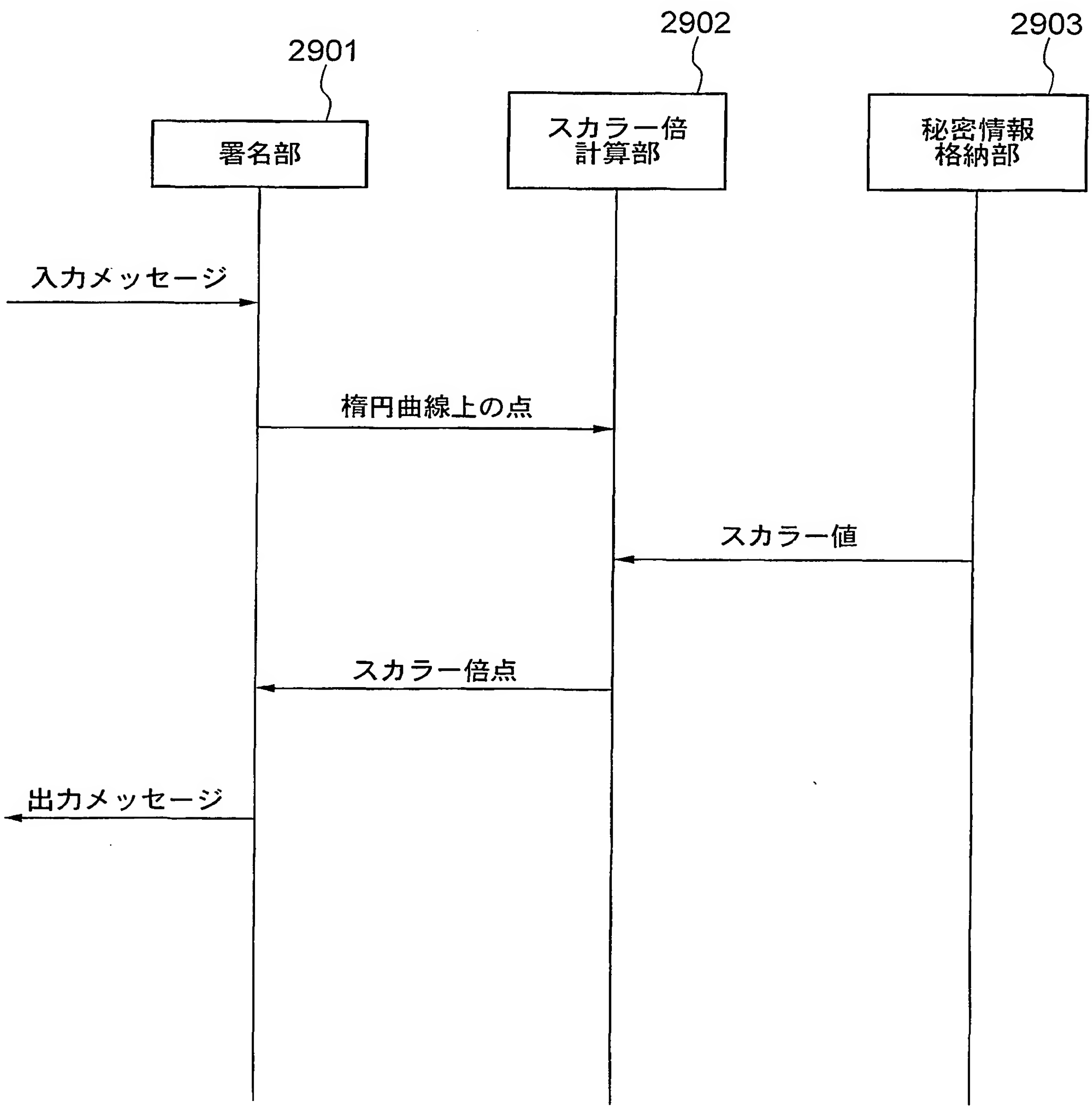

2901
2902
2903
署名部
スカラー倍
計算部
秘密情報
格納部
入力メッセージ
楕円曲線上の点
スカラー値
スカラー倍点
出力メッセージ

FIG. 30

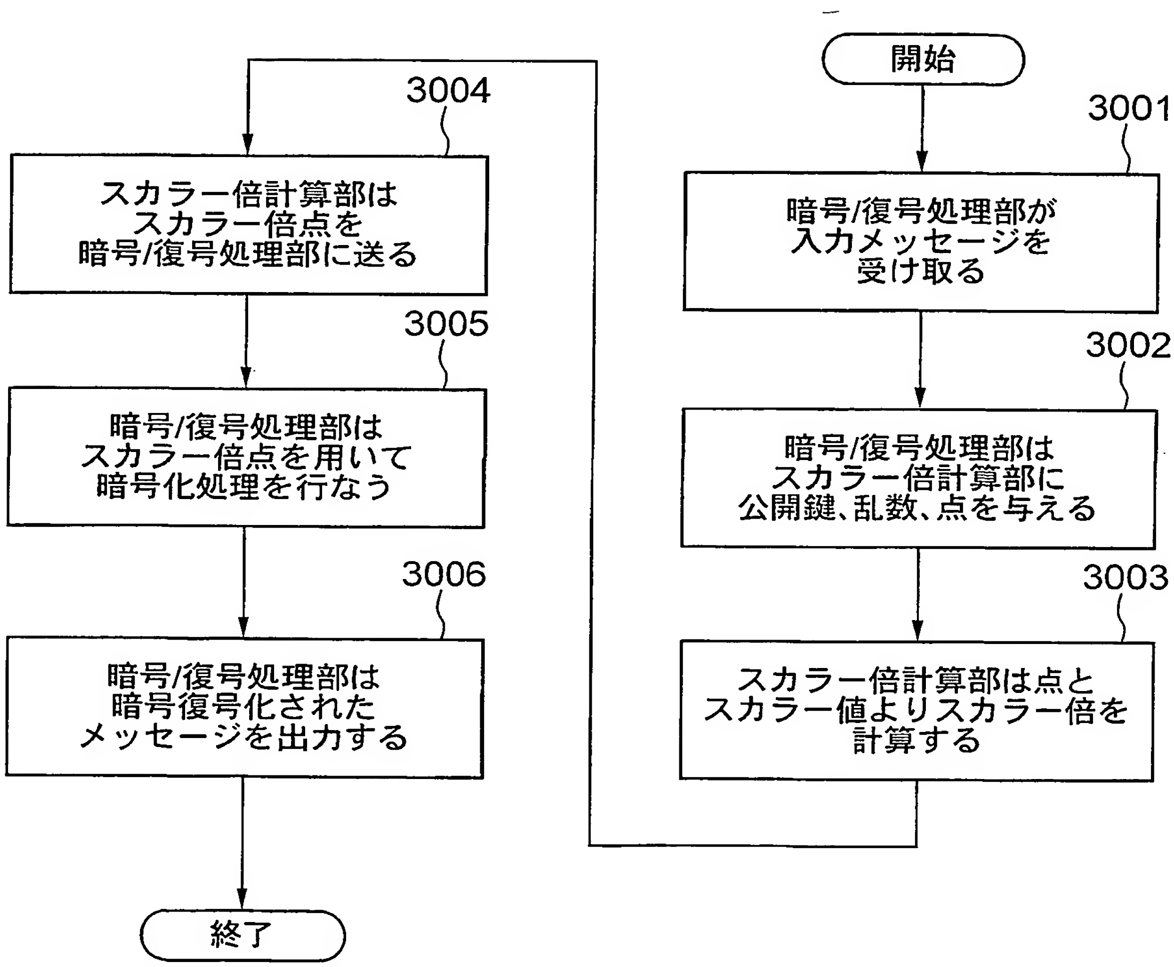

開始
3001
暗号/復号処理部が入力メッセージを受け取る
3002
暗号/復号処理部はスカラー倍計算部に公開鍵、乱数、点を与える
3003
スカラー倍計算部は点とスカラー値よりスカラー倍を計算する
3004
スカラー倍計算部はスカラー倍点を暗号/復号処理部に送る
3005
暗号/復号処理部はスカラー倍点を用いて暗号化処理を行なう
3006
暗号/復号処理部は暗号復号化されたメッセージを出力する
終了

FIG. 31

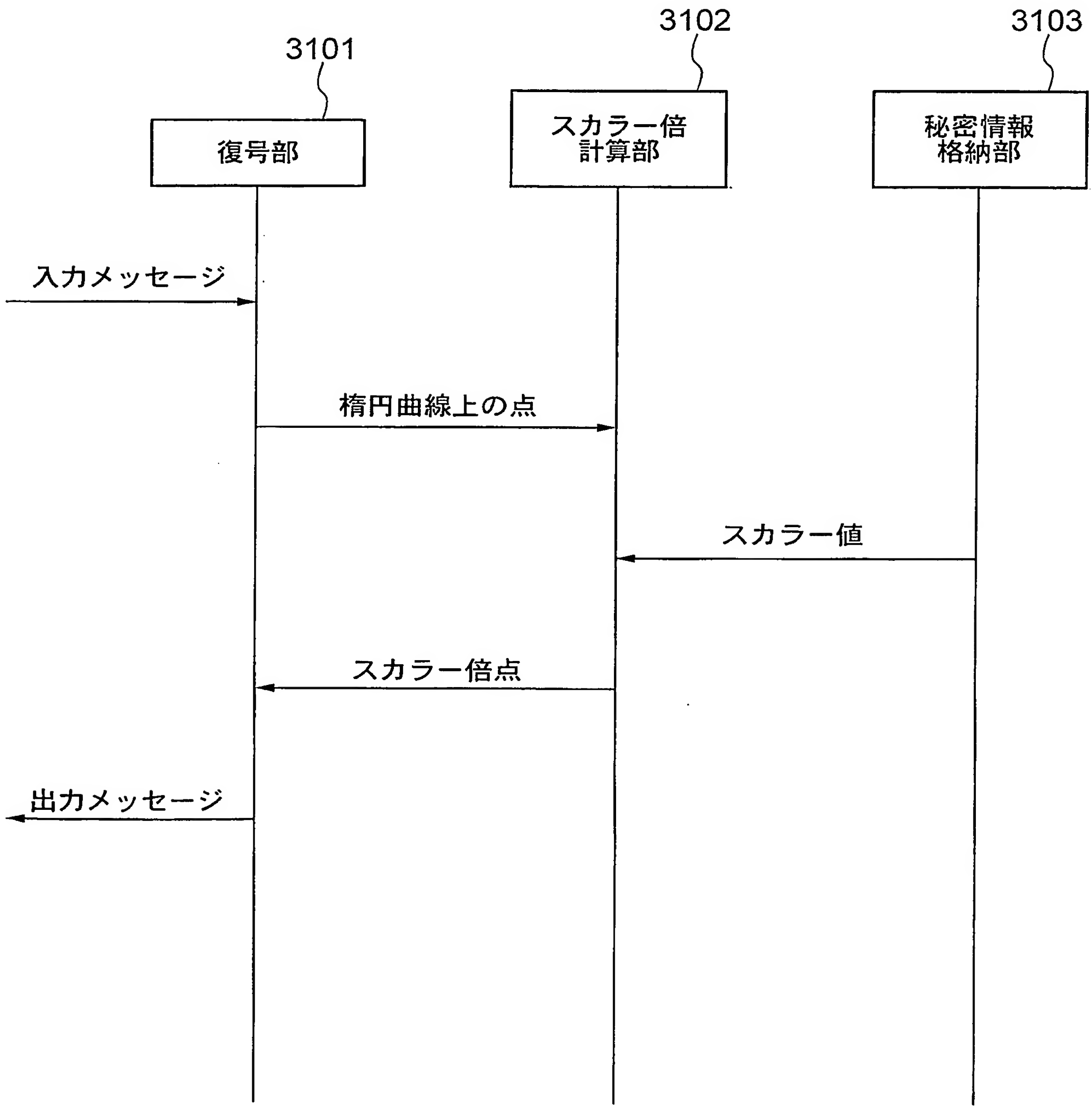

3101
3102
3103
復号部
スカラー倍計算部
秘密情報格納部
入力メッセージ
楕円曲線上の点
スカラー値
スカラー倍点
出力メッセージ

FIG. 32

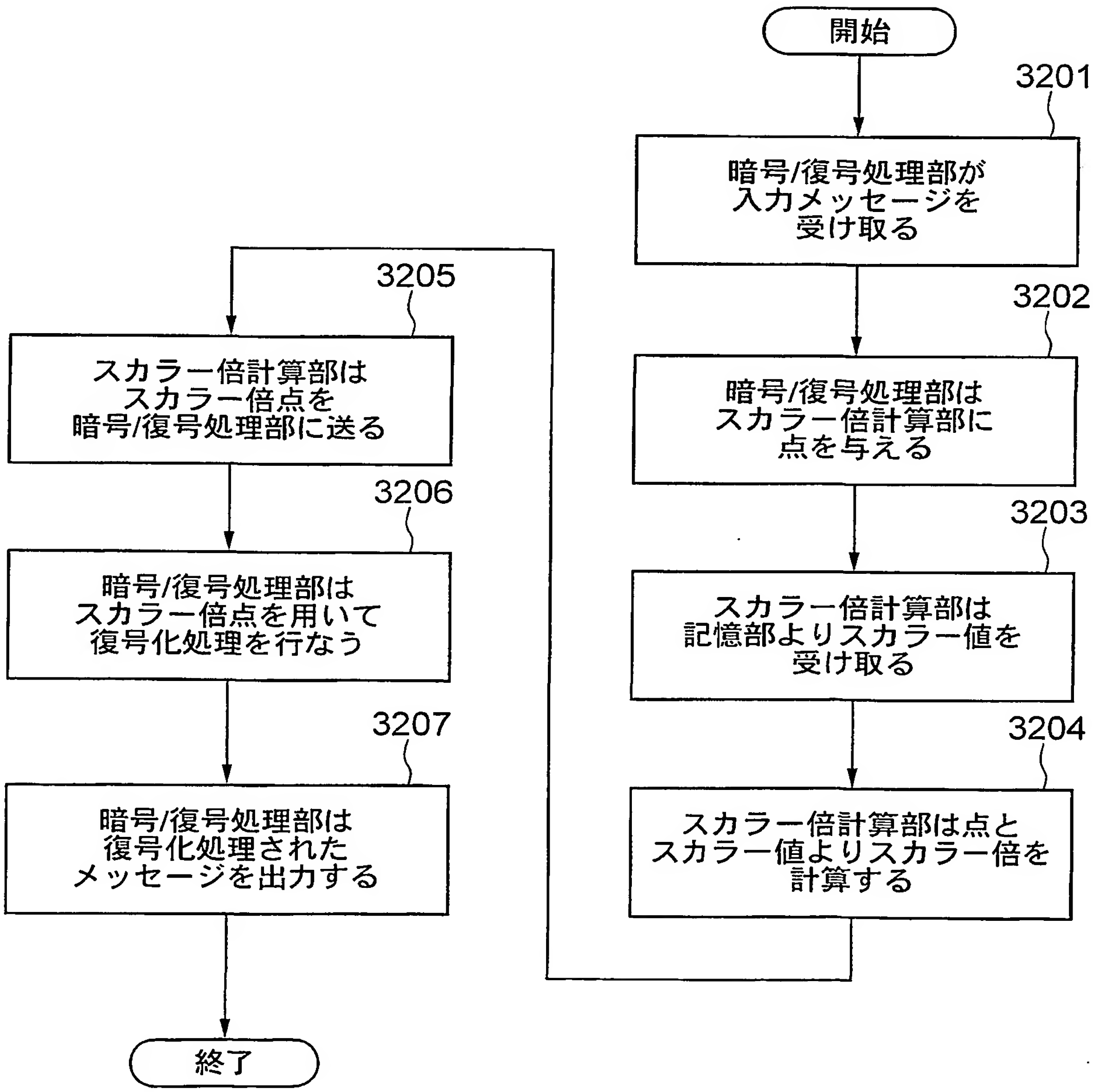

開始
3201
暗号/復号処理部が入力メッセージを受け取る
3202
暗号/復号処理部はスカラー倍計算部に点を与える
3203
スカラー倍計算部は記憶部よりスカラー値を受け取る
3204
スカラー倍計算部は点とスカラー値よりスカラー倍を計算する
3205
スカラー倍計算部はスカラー倍点を暗号/復号処理部に送る
3206
暗号/復号処理部はスカラー倍点を用いて復号化処理を行なう
3207
暗号/復号処理部は復号化処理されたメッセージを出力する
終了

FIG. 33

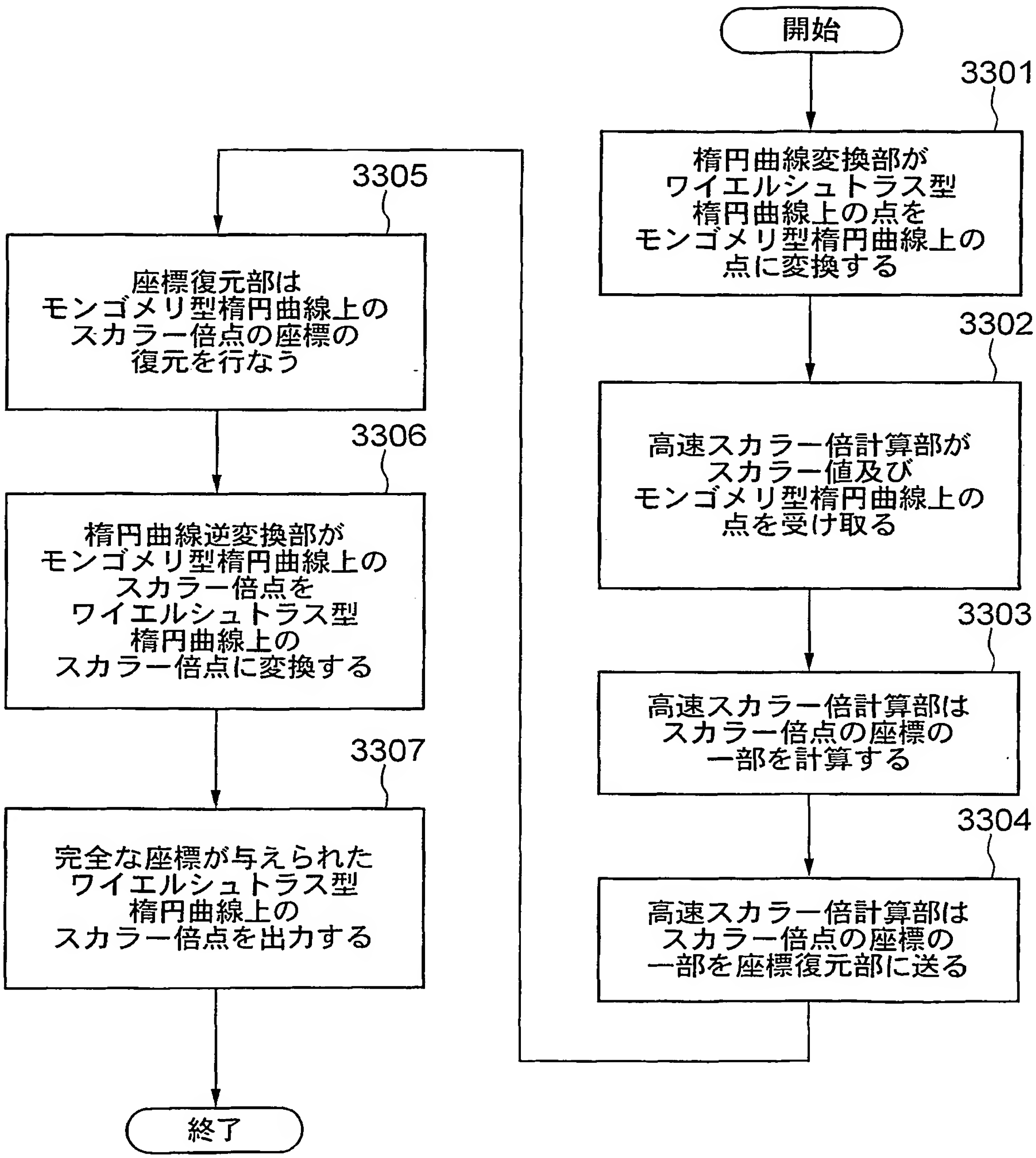

開始
3301
楕円曲線変換部が
ワイエルシュトラス型
楕円曲線上の点を
モンゴメリ型楕円曲線上の
点に変換する
3302
高速スカラー倍計算部が
スカラー値及び
モンゴメリ型楕円曲線上の
点を受け取る
3303
高速スカラー倍計算部は
スカラー倍点の座標の
一部を計算する
3304
高速スカラー倍計算部は
スカラー倍点の座標の
一部を座標復元部に送る
3305
座標復元部は
モンゴメリ型楕円曲線上の
スカラー倍点の座標の
復元を行なう
3306
楕円曲線逆変換部が
モンゴメリ型楕円曲線上の
スカラー倍点を
ワイエルシュトラス型
楕円曲線上の
スカラー倍点に変換する
3307
完全な座標が与えられた
ワイエルシュトラス型
楕円曲線上の
スカラー倍点を出力する
終了

FIG. 34

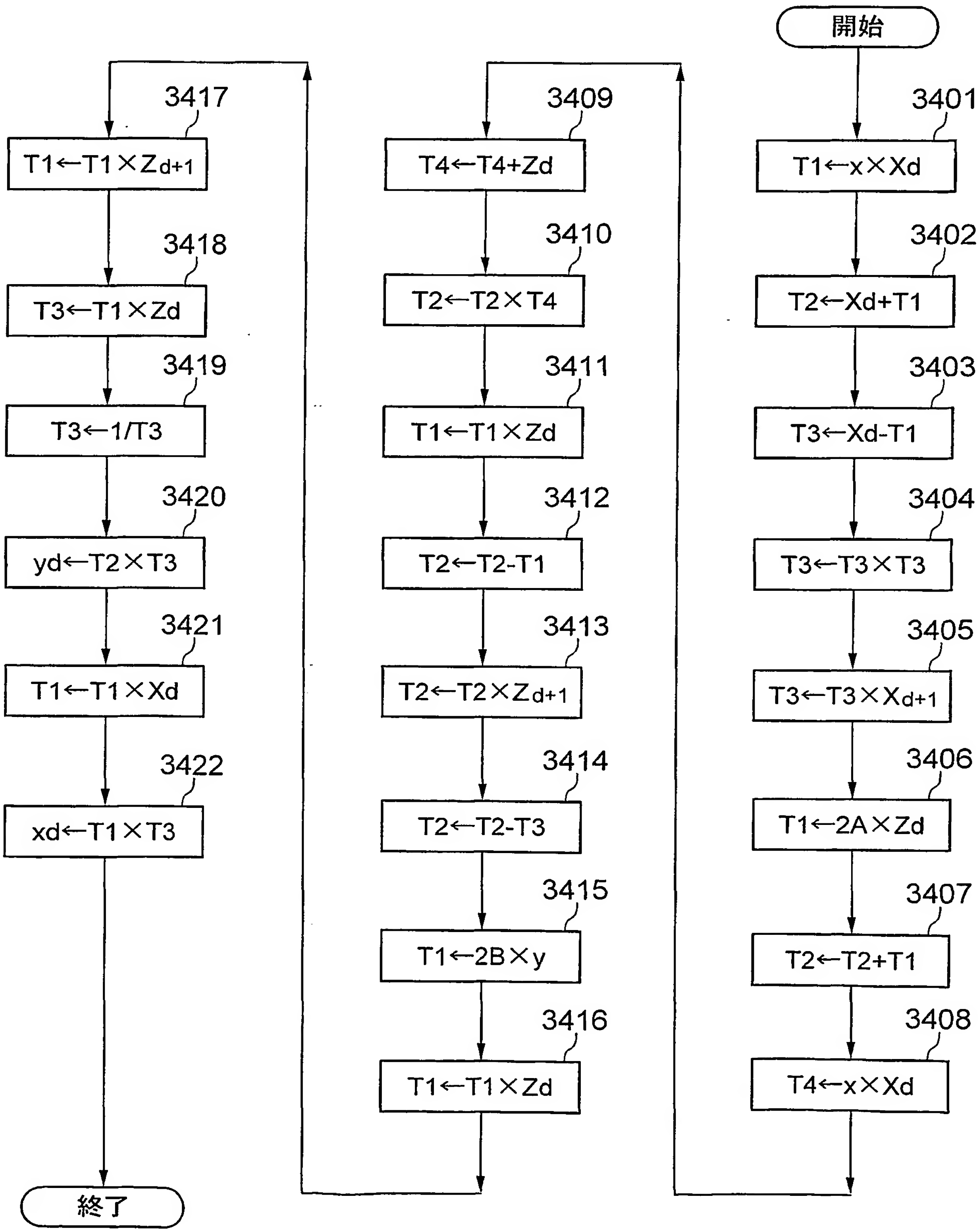

開始
3401
T1←x×Xd
3402
T2←Xd+T1
3403
T3←Xd-T1
3404
T3←T3×T3
3405
T3←T3×Xd+1
3406
T1←2A×Zd
3407
T2←T2+T1
3408
T4←x×Xd
3409
T4←T4+Zd
3410
T2←T2×T4
3411
T1←T1×Zd
3412
T2←T2-T1
3413
T2←T2×Zd+1
3414
T2←T2-T3
3415
T1←2B×y
3416
T1←T1×Zd
3417
T1←T1×Zd+1
3418
T3←T1×Zd
3419
T3←1/T3
3420
yd←T2×T3
3421
T1←T1×Xd
3422
xd←T1×T3
終了

FIG. 35

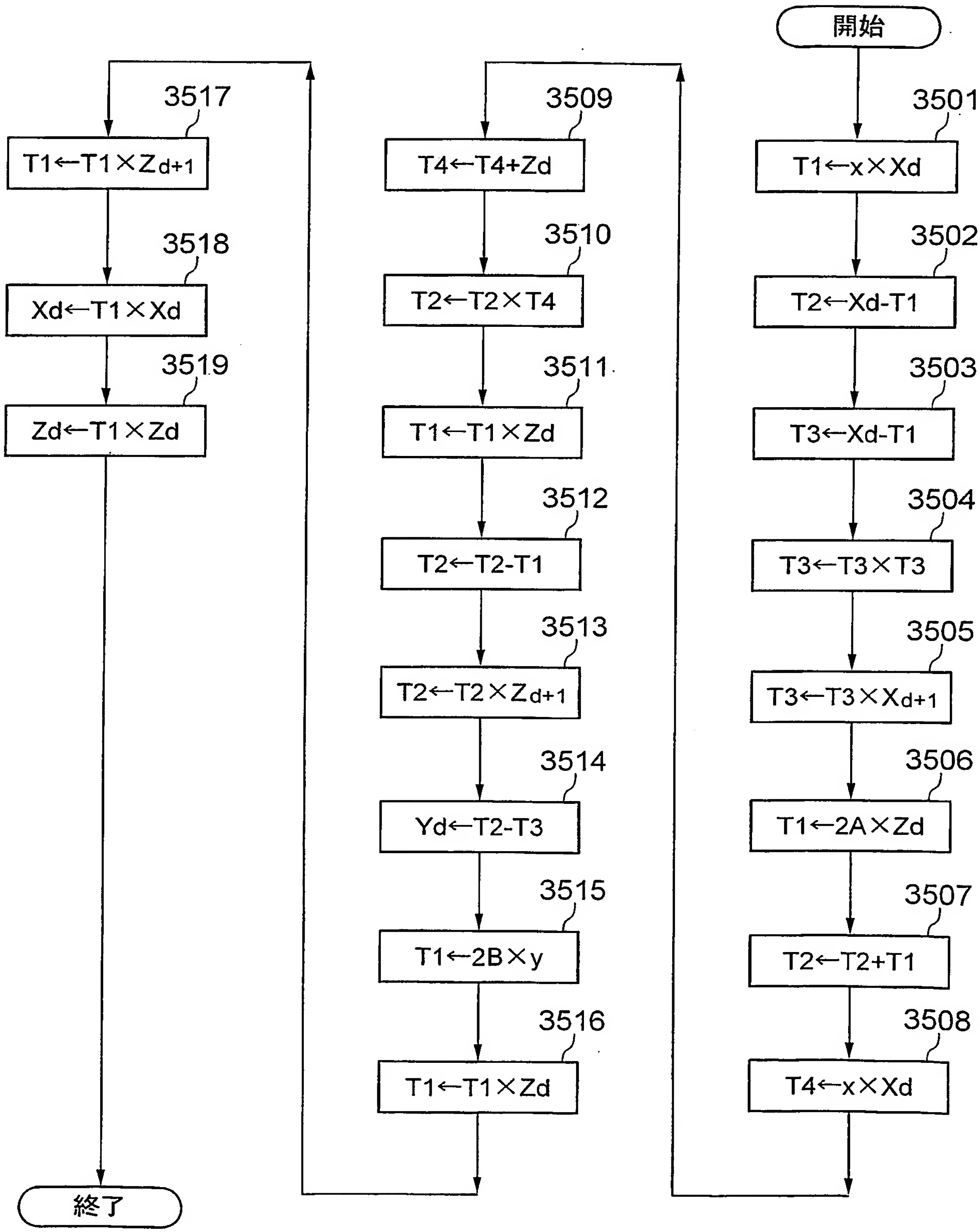

開始
3501
T1←x×Xd
3502
T2←Xd-T1
3503
T3←Xd-T1
3504
T3←T3×T3
3505
T3←T3×Xd+1
3506
T1←2A×Zd
3507
T2←T2+T1
3508
T4←x×Xd
3509
T4←T4+Zd
3510
T2←T2×T4
3511
T1←T1×Zd
3512
T2←T2-T1
3513
T2←T2×Zd+1
3514
Yd←T2-T3
3515
T1←2B×y
3516
T1←T1×Zd
3517
T1←T1×Zd+1
3518
Xd←T1×Xd
3519
Zd←T1×Zd
終了

FIG. 36

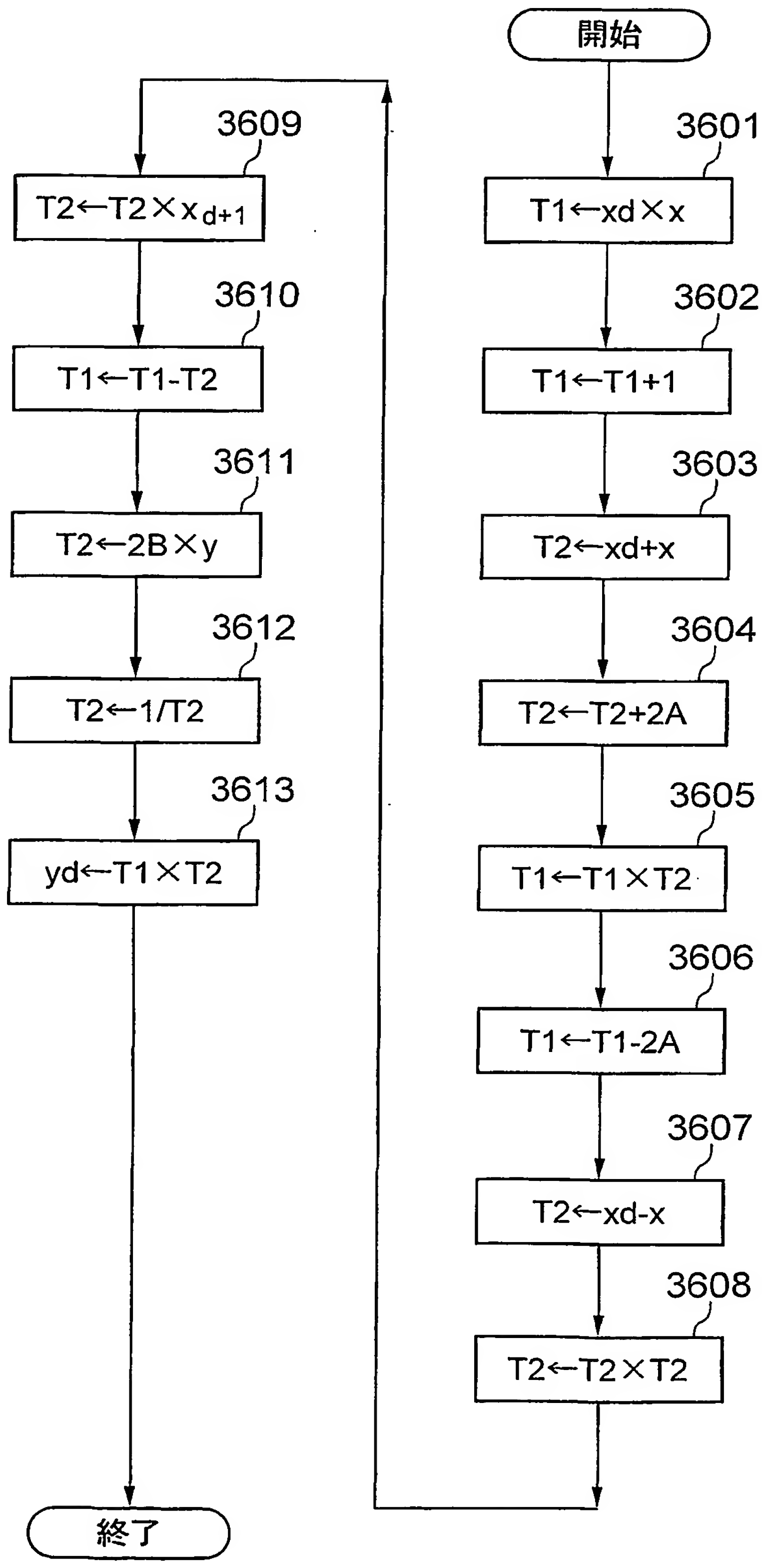
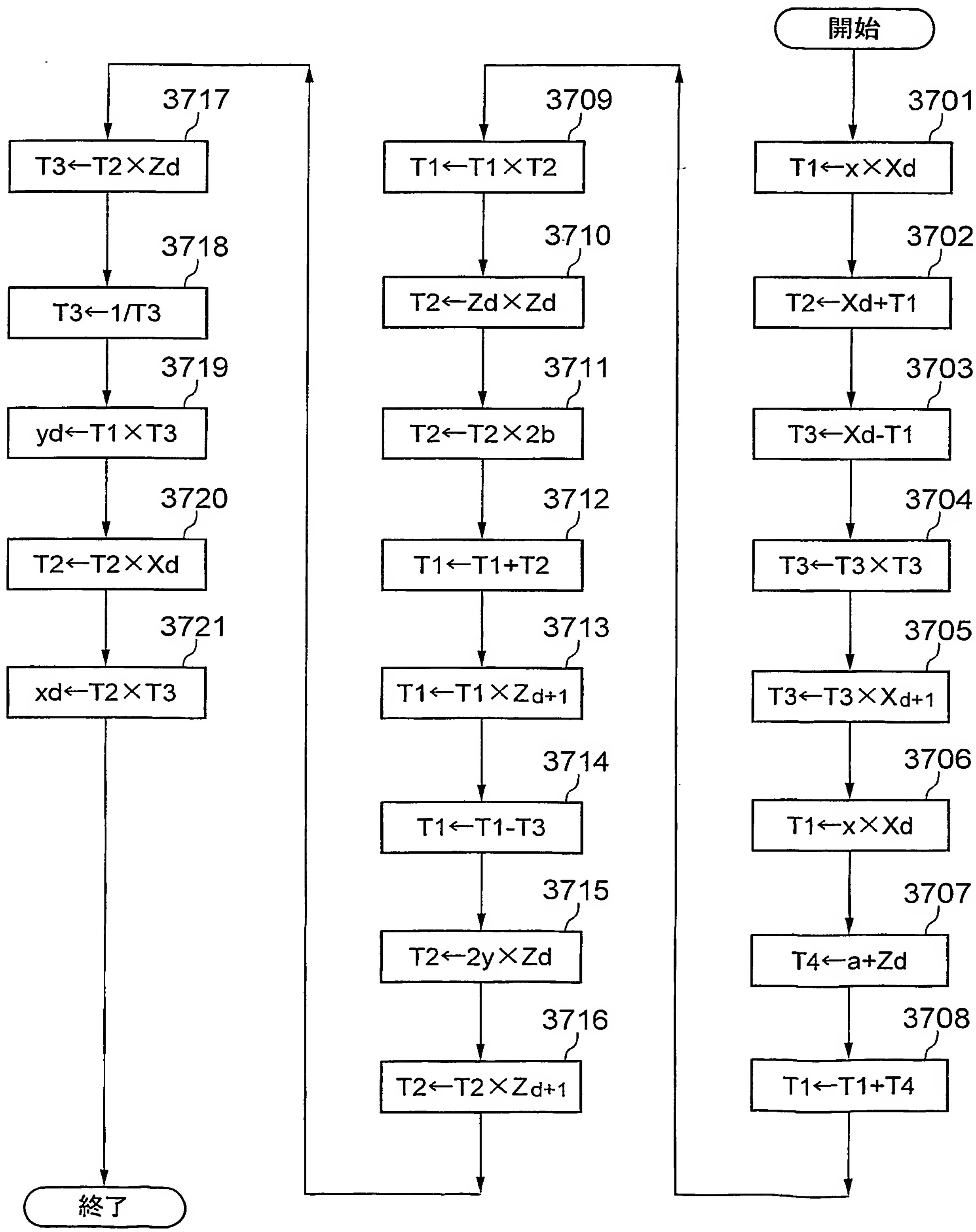

開始
3601
T1←xd×x
3602
T1←T1+1
3603
T2←xd+x
3604
T2←T2+2A
3605
T1←T1×T2
3606
T1←T1-2A
3607
T2←xd-x
3608
T2←T2×T2
3609
T2←T2×x d+1
3610
T1←T1-T2
3611
T2←2B×y
3612
T2←1/T2
3613
yd←T1×T2
終了

FIG. 37


開始
3701
T1←x×Xd
3702
T2←Xd+T1
3703
T3←Xd-T1
3704
T3←T3×T3
3705
T3←T3×Xd+1
3706
T1←x×Xd
3707
T4←a+Zd
3708
T1←T1+T4
3709
T1←T1×T2
3710
T2←Zd×Zd
3711
T2←T2×2b
3712
T1←T1+T2
3713
T1←T1×Zd+1
3714
T1←T1-T3
3715
T2←2y×Zd
3716
T2←T2×Zd+1
3717
T3←T2×Zd
3718
T3←1/T3
3719
yd←T1×T3
3720
T2←T2×Xd
3721
xd←T2×T3
終了

# FIG. 38

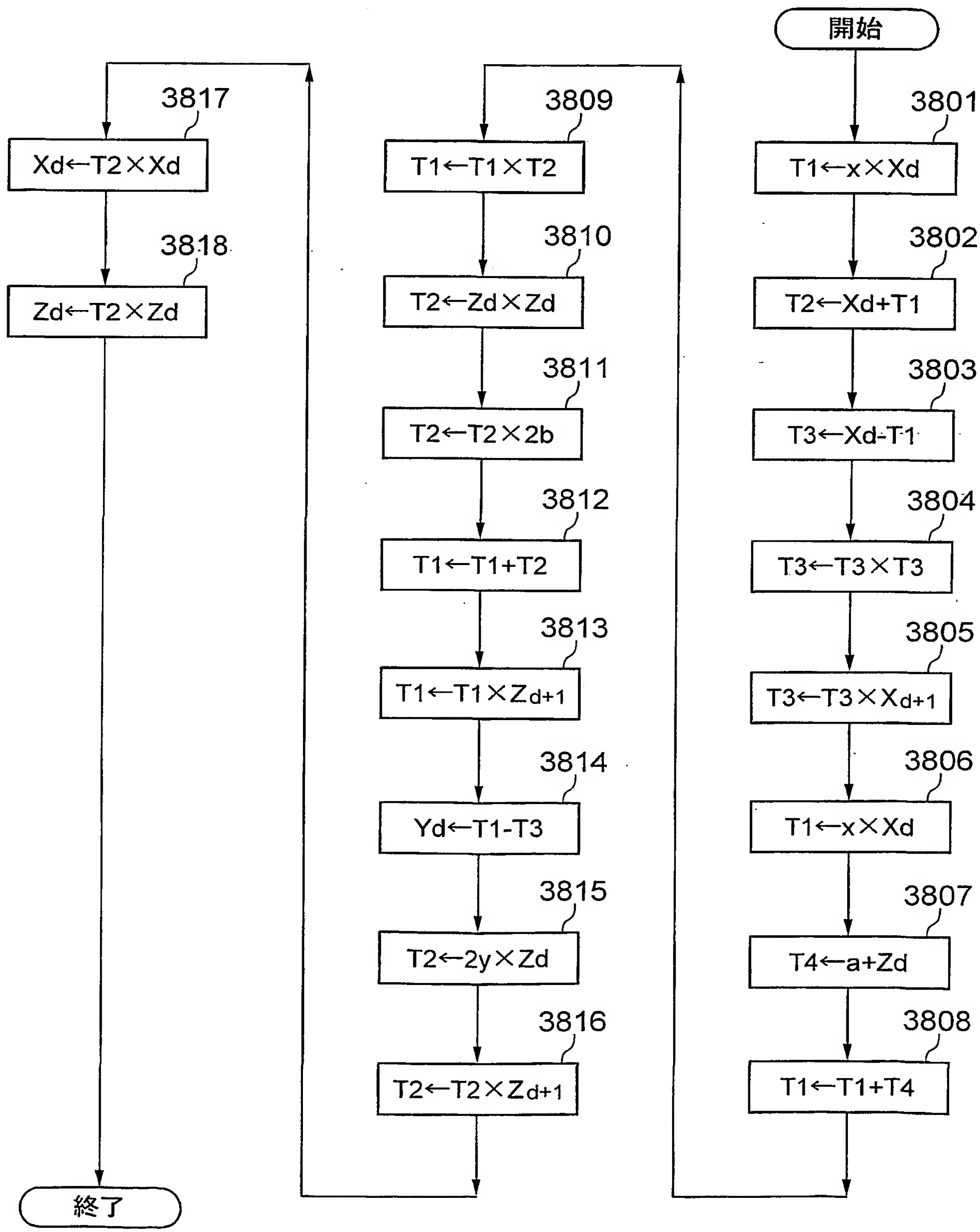
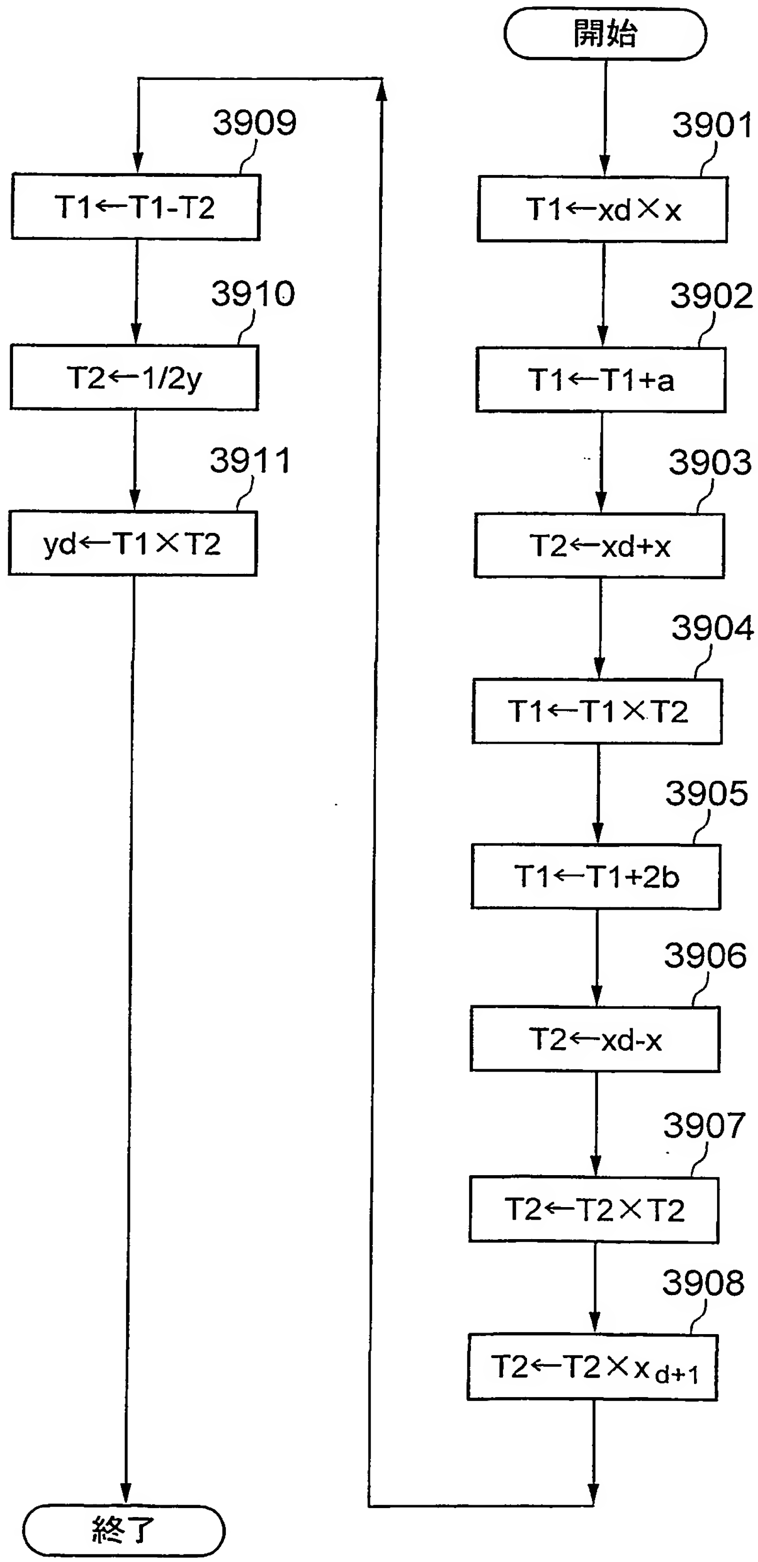
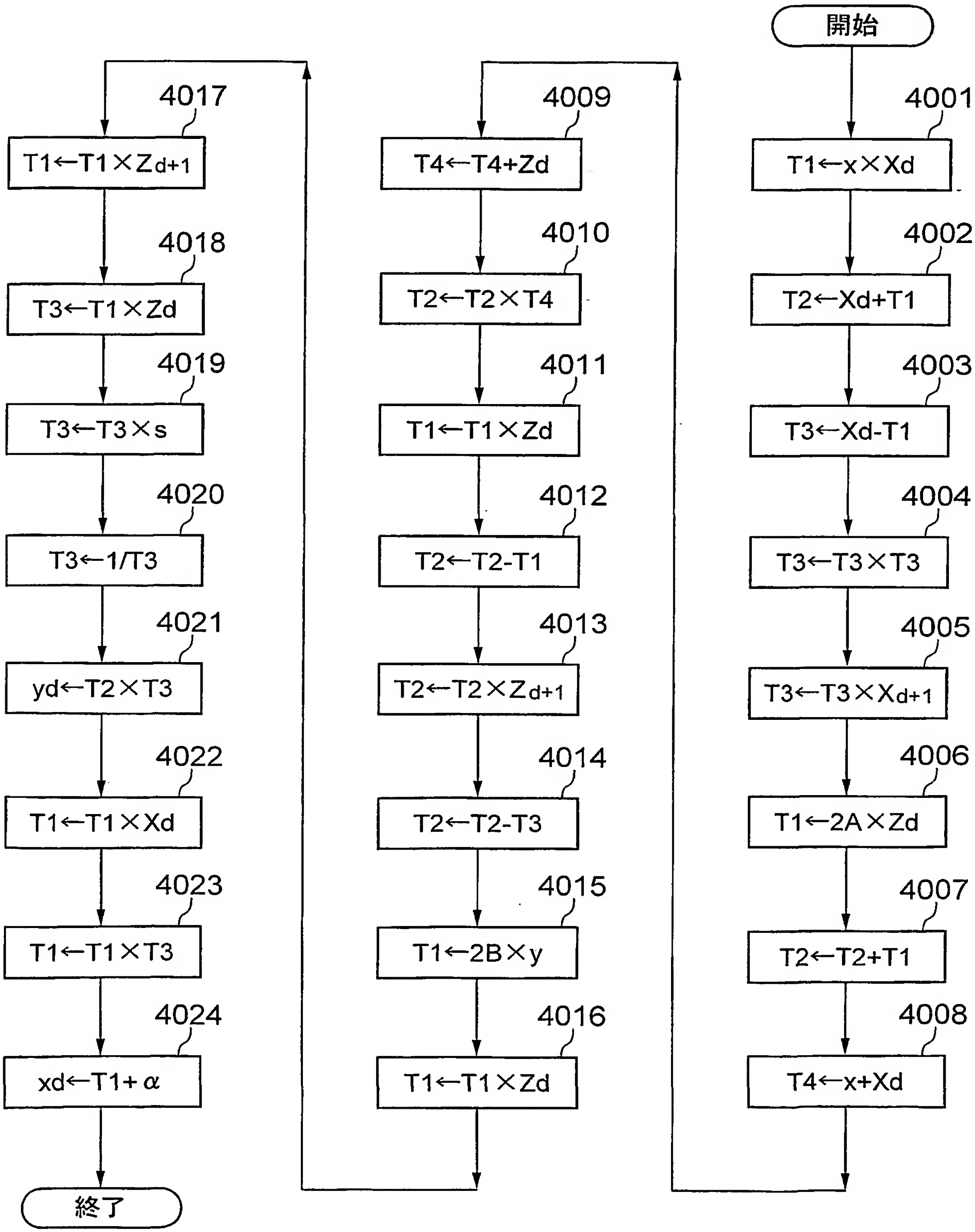

開始
3801
T1←x×Xd
3802
T2←Xd+T1
3803
T3←Xd-T1
3804
T3←T3×T3
3805
T3←T3×Xd+1
3806
T1←x×Xd
3807
T4←a+Zd
3808
T1←T1+T4
3809
T1←T1×T2
3810
T2←Zd×Zd
3811
T2←T2×2b
3812
T1←T1+T2
3813
T1←T1×Zd+1
3814
Yd←T1-T3
3815
T2←2y×Zd
3816
T2←T2×Zd+1
3817
Xd←T2×Xd
3818
Zd←T2×Zd
終了

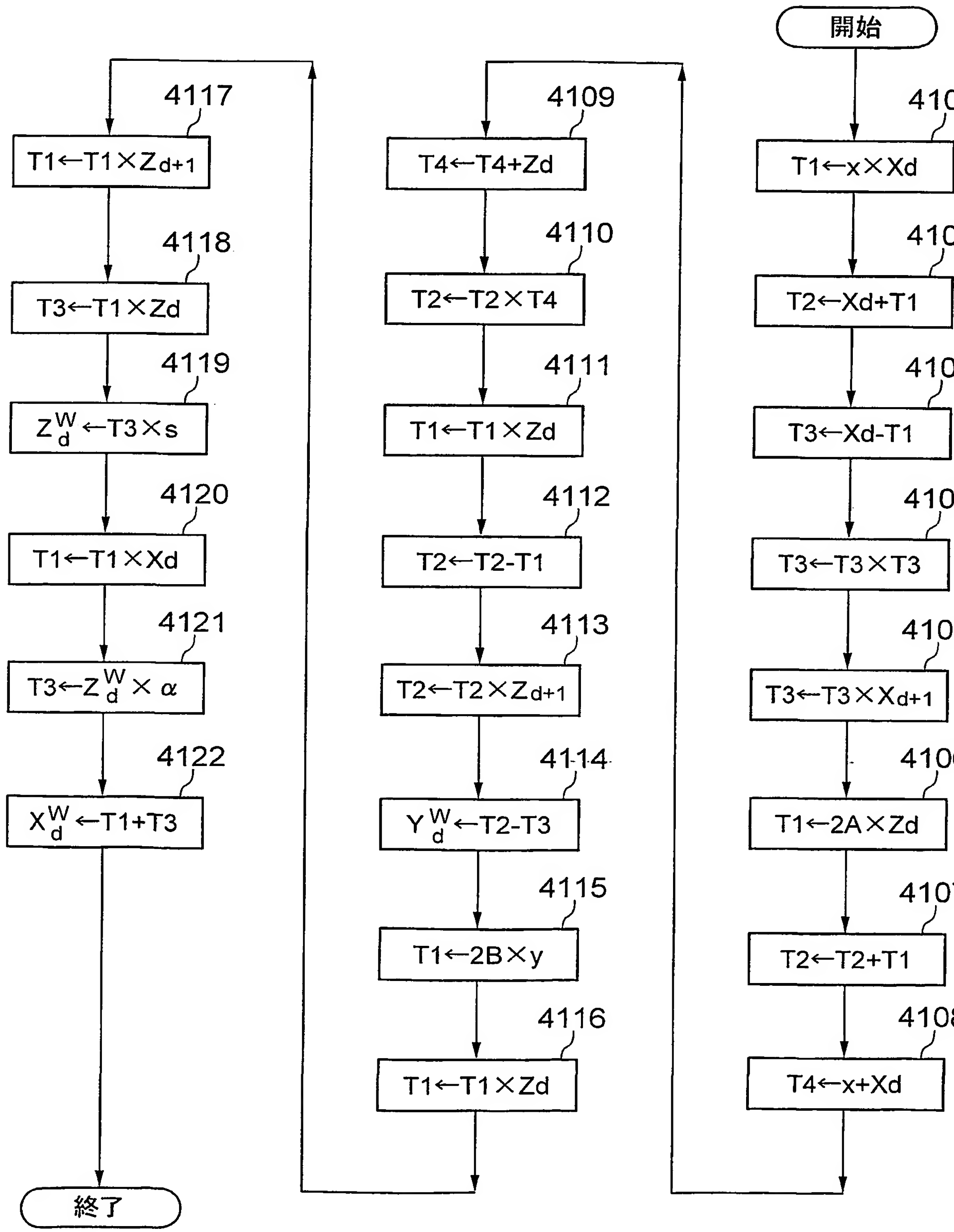
FIG. 39


開始
3901
T1←xd×x
3902
T1←T1+a
3903
T2←xd+x
3904
T1←T1×T2
3905
T1←T1+2b
3906
T2←xd-x
3907
T2←T2×T2
3908
T2←T2×x d+1
3909
T1←T1-T2
3910
T2←1/2y
3911
yd←T1×T2
終了

# FIG. 40


開始
4001
T1←x×Xd
4002
T2←Xd+T1
4003
T3←Xd-T1
4004
T3←T3×T3
4005
T3←T3×Xd+1
4006
T1←2A×Zd
4007
T2←T2+T1
4008
T4←x+Xd
4009
T4←T4+Zd
4010
T2←T2×T4
4011
T1←T1×Zd
4012
T2←T2-T1
4013
T2←T2×Zd+1
4014
T2←T2-T3
4015
T1←2B×y
4016
T1←T1×Zd
4017
T1←T1×Zd+1
4018
T3←T1×Zd
4019
T3←T3×s
4020
T3←1/T3
4021
yd←T2×T3
4022
T1←T1×Xd
4023
T1←T1×T3
4024
xd←T1+α
終了

# FIG. 41


開始
4101
T1←x×Xd
4102
T2←Xd+T1
4103
T3←Xd-T1
4104
T3←T3×T3
4105
T3←T3×Xd+1
4106
T1←2A×Zd
4107
T2←T2+T1
4108
T4←x+Xd
4109
T4←T4+Zd
4110
T2←T2×T4
4111
T1←T1×Zd
4112
T2←T2-T1
4113
T2←T2×Zd+1
4114
Y W d←T2-T3
4115
T1←2B×y
4116
T1←T1×Zd
4117
T1←T1×Zd+1
4118
T3←T1×Zd
4119
Z W d←T3×s
4120
T1←T1×Xd
4121
T3←Z W d×α
4122
X W d←T1+T3
終了

# FIG. 42

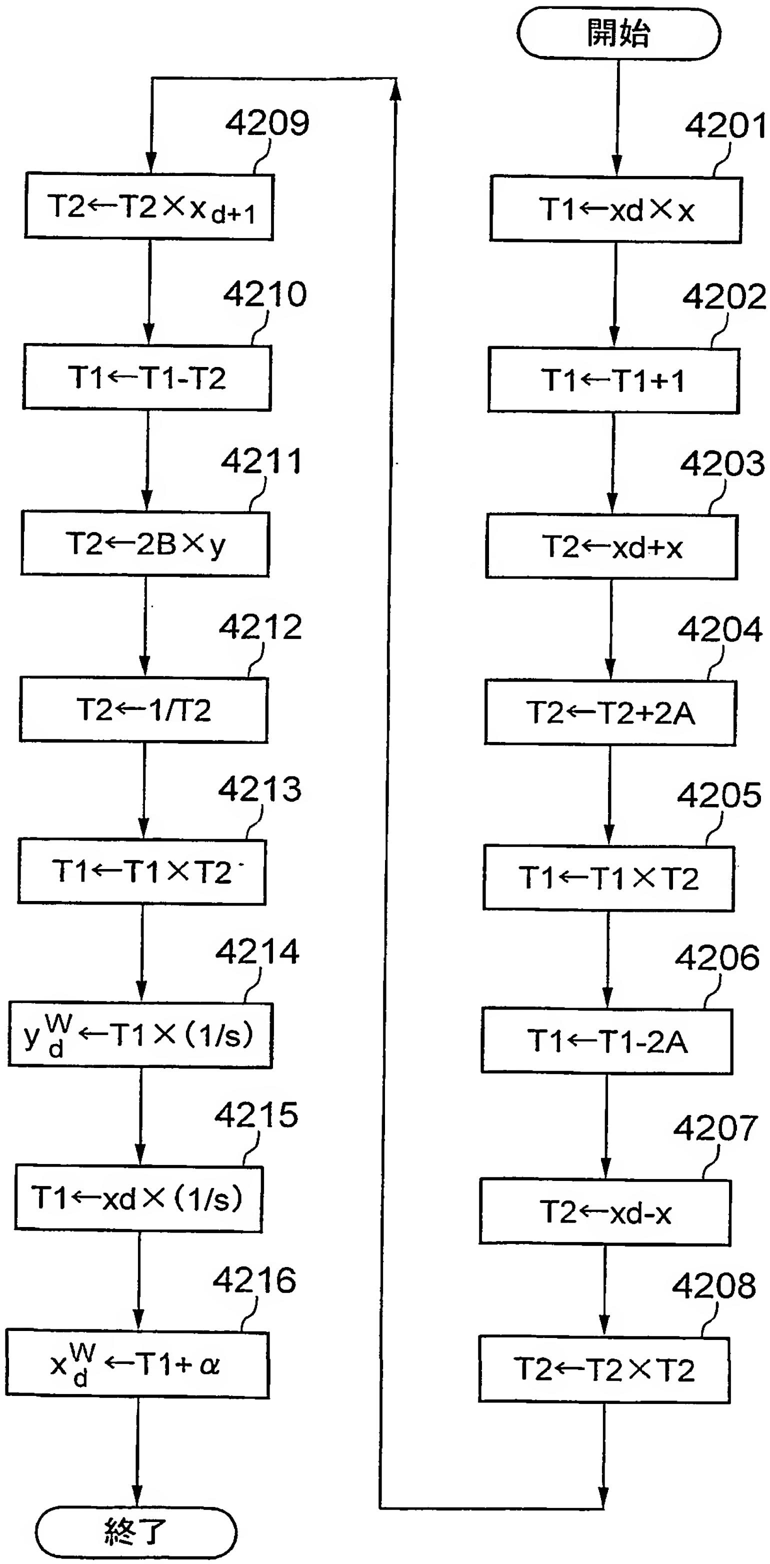
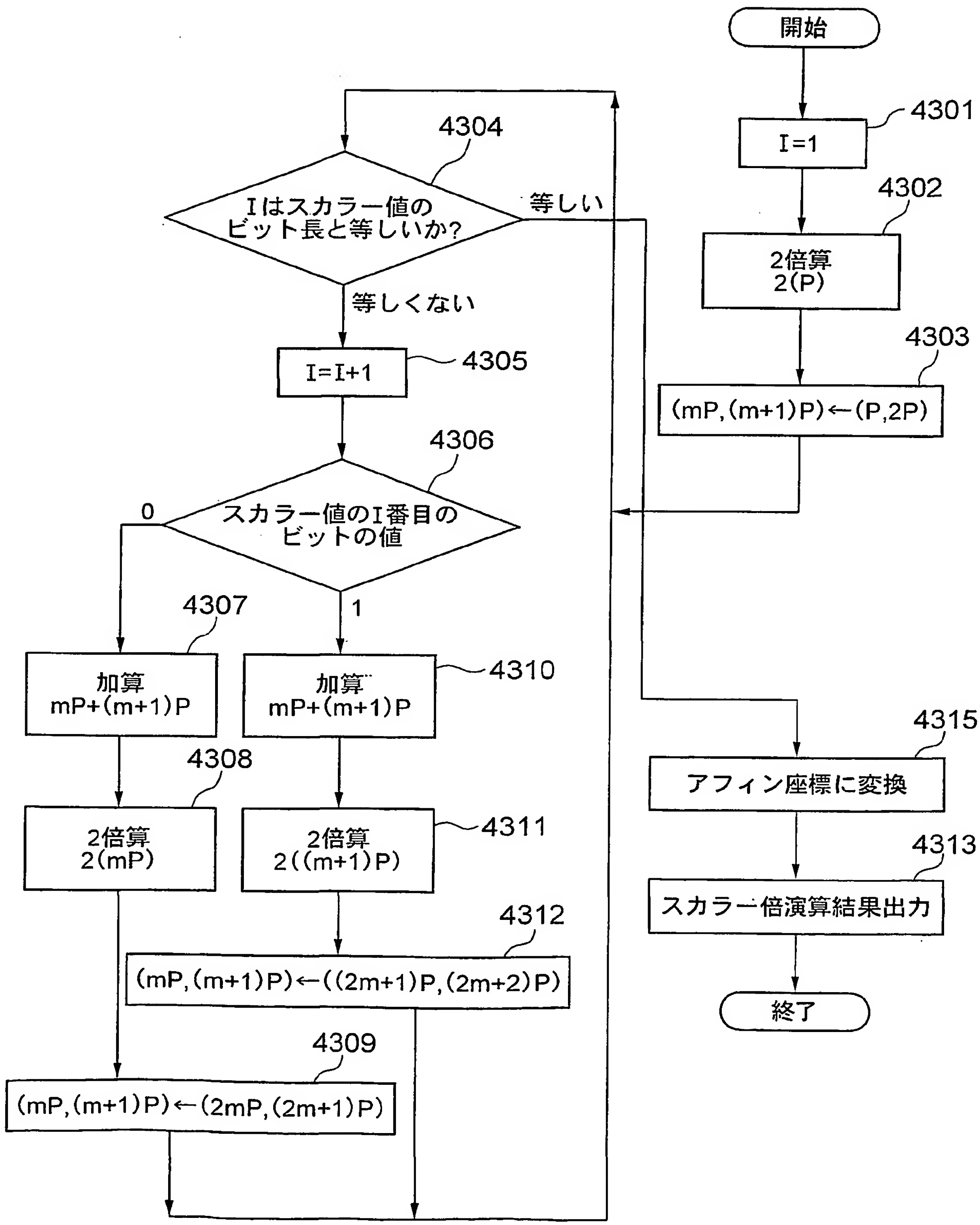

開始
4201
T1←xd×x
4202
T1←T1+1
4203
T2←xd+x
4204
T2←T2+2A
4205
T1←T1×T2
4206
T1←T1-2A
4207
T2←xd-x
4208
T2←T2×T2
4209
T2←T2×x d+1
4210
T1←T1-T2
4211
T2←2B×y
4212
T2←1/T2
4213
T1←T1×T2
4214
$y_d^W$←T1×(1/s)
4215
T1←xd×(1/s)
4216
$x_d^W$←T1+α
終了

FIG. 43



開始
4301
I=1
4302
2倍算
2(P)
4303
(mP,(m+1)P)←(P,2P)
4304
Iはスカラー値のビット長と等しいか?
等しい
等しくない
4305
I=I+1
4306
スカラー値のI番目のビットの値
0
1
4307
加算
mP+(m+1)P
4310
加算
mP+(m+1)P
4308
2倍算
2(mP)
4311
2倍算
2((m+1)P)
4312
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
4309
(mP,(m+1)P)←(2mP,(2m+1)P)
4315
アフィン座標に変換
4313
スカラー倍演算結果出力
終了

FIG. 44

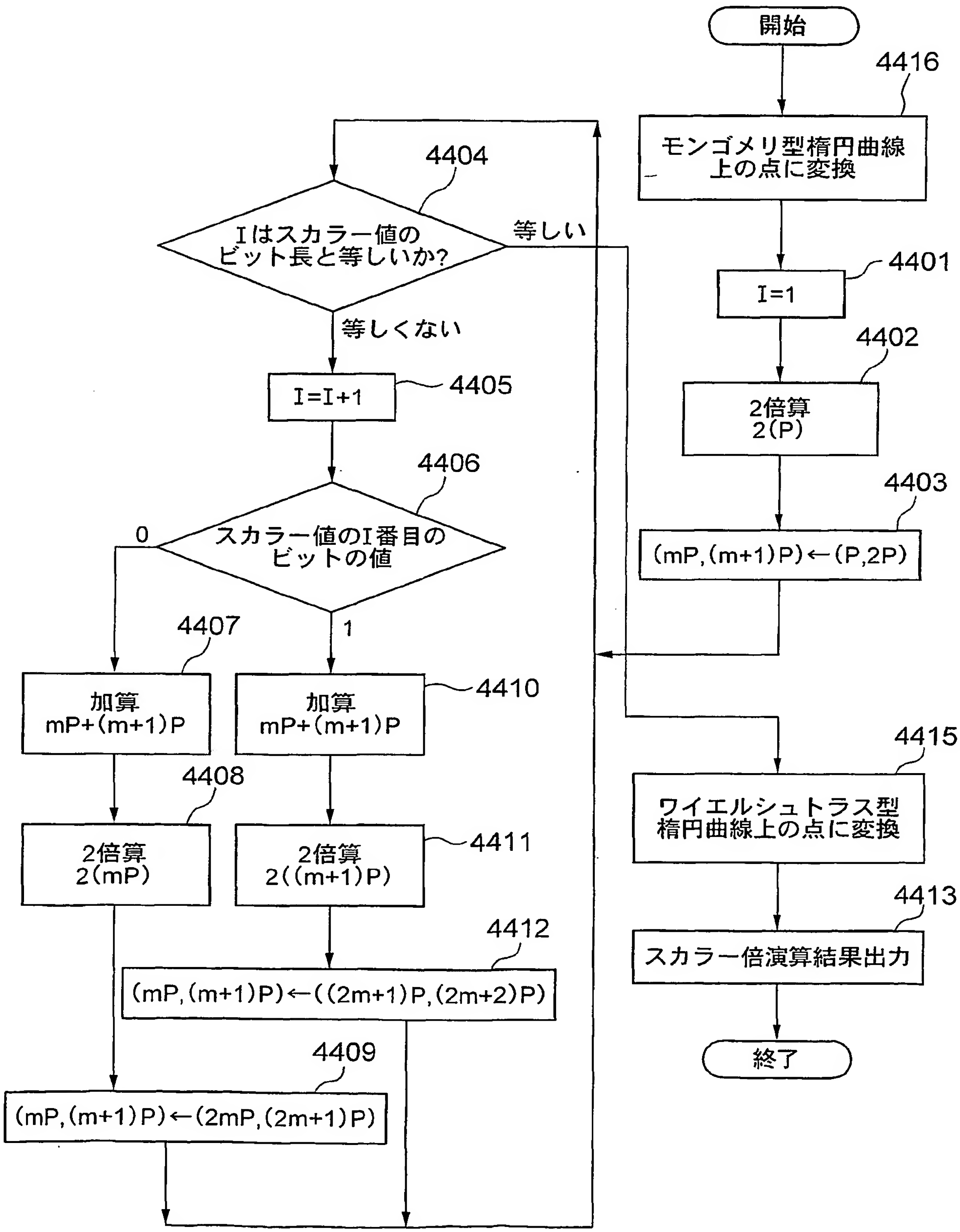
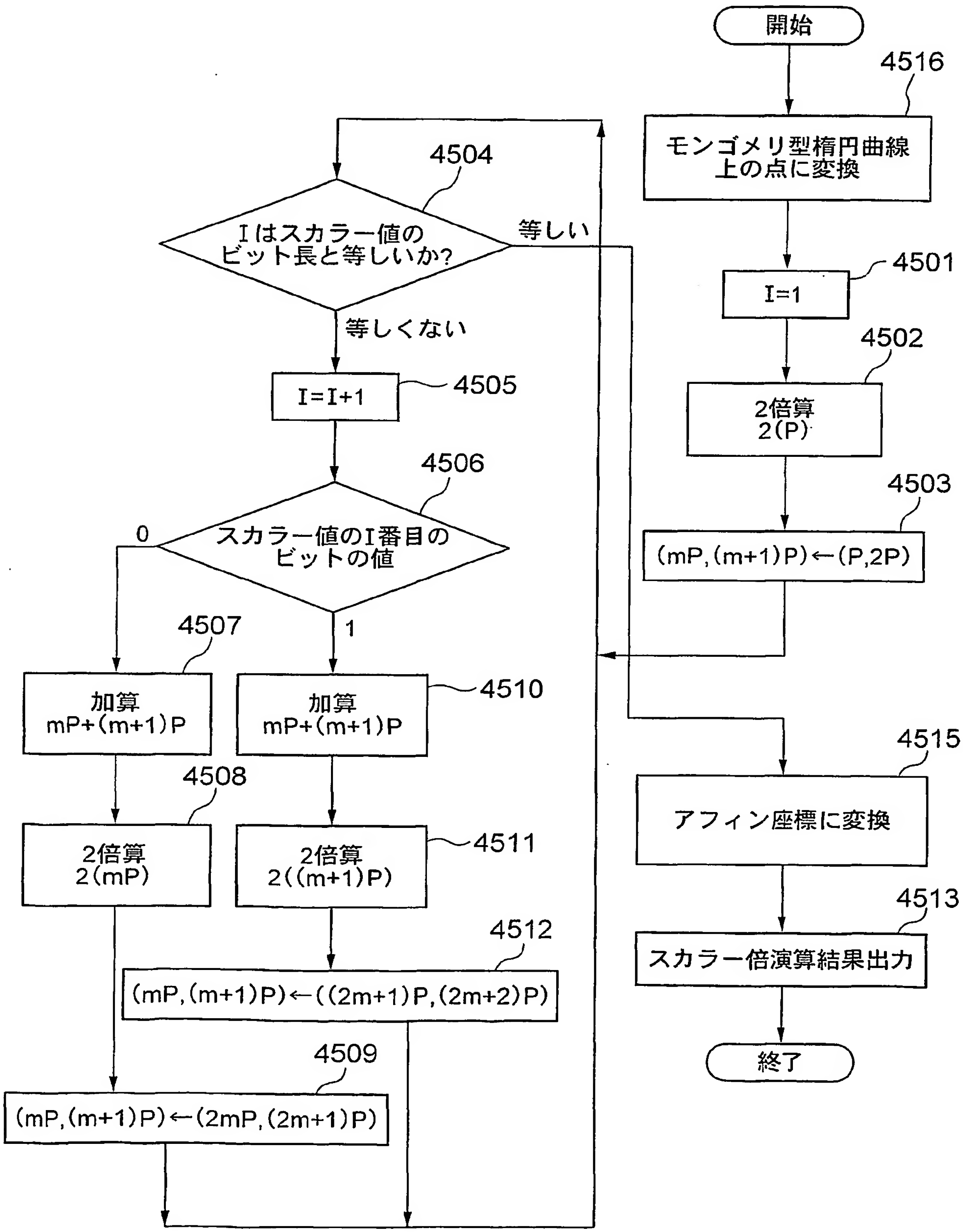

開始
4416
モンゴメリ型楕円曲線上の点に変換
4401
I=1
4402
2倍算
2(P)
4403
(mP,(m+1)P)←(P,2P)
4404
Iはスカラー値のビット長と等しいか?
等しい
等しくない
4405
I=I+1
4406
スカラー値のI番目のビットの値
0
1
4407
加算
mP+(m+1)P
4410
加算
mP+(m+1)P
4408
2倍算
2(mP)
4411
2倍算
2((m+1)P)
4412
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
4409
(mP,(m+1)P)←(2mP,(2m+1)P)
4415
ワイエルシュトラス型楕円曲線上の点に変換
4413
スカラー倍演算結果出力
終了

FIG. 45


開始
4516
モンゴメリ型楕円曲線上の点に変換
4501
I=1
4502
2倍算
2(P)
4503
(mP,(m+1)P)←(P,2P)
4504
Iはスカラー値のビット長と等しいか?
等しい
等しくない
4505
I=I+1
4506
スカラー値のI番目のビットの値
0
1
4507
加算
mP+(m+1)P
4508
2倍算
2(mP)
4509
(mP,(m+1)P)←(2mP,(2m+1)P)
4510
加算
mP+(m+1)P
4511
2倍算
2((m+1)P)
4512
(mP,(m+1)P)←((2m+1)P,(2m+2)P)
4515
アフィン座標に変換
4513
スカラー倍演算結果出力
終了

PATENT COOPERATION TREATY

# PCT

## DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13*ter*.1(c) and 39)

| Applicant's or agent's file reference<br>E6369-00 | **IMPORTANT DECLARATION** | Date of mailing *(day/month/year)*<br>11 December, 2001 (11.12.01) |
|---|---|---|
| International application No.<br>PCT/JP01/09781 | International filing date *(day/month/year)*<br>08 November, 2001 (08.11.01) | (Earliest) Priority Date *(day/month/year)*<br>08 November, 2000 (08.11.00) |
| International Patent Classification (IPC) or both national classification and IPC<br>Int. Cl7 H04L9/30, G09C1/00 | | |
| Applicant<br>Hitachi, Ltd. | | |

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. ☒ The subject matter of the international application relates to:
   - a. ☐ scientific theories.
   - b. ☒ mathematical theories.
   - c. ☐ plant varieties.
   - d. ☐ animal varieties.
   - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. ☐ schemes, rules or methods of doing business.
   - g. ☐ schemes, rules or methods of performing purely mental acts.
   - h. ☐ schemes, rules or methods of playing games.
   - i. ☐ methods for treatment of the human body by surgery or therapy.
   - j. ☐ methods for treatment of the animal body by surgery or therapy.
   - k. ☐ diagnostic methods practised on the human or animal body.
   - l. ☐ mere presentations of information.
   - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.
2. ☐ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
   ☐ the description ☐ the claims ☐ the drawings
3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:
   - ☐ the written form has not been furnished or does not comply with the standard.
   - ☐ the computer readable form has not been furnished or does not comply with the standard.
4. Further comments:

| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br><br>Telephone No. |
|---|---|

Form PCT/ISA/203 (July 1998)

特　許　協　力　条　約

PCT

# 国際調査報告を作成しない旨の決定

（法第８条第２項、法施行規則第42条、第50条の3第
〔ＰＣＴ17条(2)(a)、ＰＣＴ規則13の3.1(c)、39〕

| | | |
|---|---|---|
| 出願人又は代理人の書類記号　Ｅ６３６９－００ | 重要決定 | 発送日（日.月.年）　11.12.01 |
| 国際出願番号　ＰＣＴ／ＪＰ０１／０９７８１ | 国際出願日（日.月.年）　０８．１１．０１ | 優先日（日.月.年）　０８．１１．００ |
| 国際特許分類（ＩＰＣ）　Ｉｎｔ．Ｃｌ$^7$　Ｈ０４Ｌ９／３０，Ｇ０９Ｃ１／００ | | |
| 出願人（氏名又は名称）　株式会社　日立製作所 | | |

この出願については、法第８条第２項（ＰＣＴ17条(2)(a)）の規定に基づき、次の理由により国際調査報告を作成しない旨の決定をする。

1. [X] この国際出願は、次の事項を内容としている。
   - a. [ ] 科学の理論
   - b. [X] 数学の理論
   - c. [ ] 植物の品種
   - d. [ ] 動物の品種
   - e. [ ] 植物及び動物の生産の本質的に生物学的な方法（微生物学的方法による生産物及び微生物学的方法を除く。）
   - f. [ ] 事業活動に関する計画、法則又は方法
   - g. [ ] 純粋に精神的な行為の遂行に関する計画、法則又は方法
   - h. [ ] 遊戯に関する計画、法則又は方法
   - i. [ ] 人の身体の手術又は治療による処置方法
   - j. [ ] 動物の身体の手術又は治療による処置方法
   - k. [ ] 人又は動物の身体の診断方法
   - l. [ ] 情報の単なる提示
   - m. [ ] この国際調査機関が先行技術を調査できないコンピューター・プログラム
2. [ ] この国際出願の次の部分が所定の要件を満たしていないので、有効な国際調査をすることができない。
   [ ] 明細書　[ ] 請求の範囲　[ ] 図面
3 [ ] ヌクレオチド又はアミノ酸の配列表が実施細則の附属書Ｃ（塩基配列又はアミノ酸配列を含む明細書等の作成のためのガイドライン）に定める基準を満たしていないので、有効な国際調査をすることができない。
   [ ] 書面による配列表が提出されていない又は所定の基準を満たしていない。
   [ ] フレキシブルディスクによる配列表が提出されていない又は所定の基準を満たしていない。
4. 附記

| | | |
|---|---|---|
| 名称及びあて名<br>日本国特許庁（ＩＳＡ／ＪＰ）<br>郵便番号１００－８９１５<br>東京都千代田区霞が関三丁目４番３号 | 特許庁審査官（権限のある職員）<br>中里　裕正<br>電話番号　０３－３５８１－１１０１　内線　３５９７ | ５Ｍ　９３６４ |

様式ＰＣＴ／ＩＳＡ／２０３（１９９８年７月）

PCT
08.11.01
受領印



E6369-00

特許協力条約に基づく国際出願願書
原本（出願用）- 印刷日時 2001年11月08日 (08.11.2001) 木曜日 09時37分12秒

| | | |
|---|---|---|
| 0 | 受理官庁記入欄 | |
| 0-1 | 国際出願番号. | |
| 0-2 | 国際出願日 | |
| 0-3 | (受付印) | |
| 0-4 | 様式-PCT/RO/101<br>この特許協力条約に基づく国際出願願書は、 | |
| 0-4-1 | 右記によって作成された。 | PCT-EASY Version 2.92<br>(updated 01.03.2001) |
| 0-5 | 申立て<br>出願人は、この国際出願が特許協力条約に従って処理されることを請求する。 | |
| 0-6 | 出願人によって指定された受理官庁 | 日本国特許庁 (RO/JP) |
| 0-7 | 出願人又は代理人の書類記号 | E6369-00 |
| I | 発明の名称 | 楕円曲線スカラー倍計算方法及び装置並びに記憶媒体 |
| II | 出願人 | |
| II-1 | この欄に記載した者は | 出願人である (applicant only) |
| II-2 | 右の指定国についての出願人である。 | 米国を除くすべての指定国 (all designated States except US) |
| II-4ja | 名称 | 株式会社　日立製作所 |
| II-4en | Name | HITACHI, LTD. |
| II-5ja | あて名: | 101-8010 日本国<br>東京都 千代田区<br>神田駿河台四丁目６番地 |
| II-5en | Address: | 6, Kanda surugadai 4-chome,<br>Chiyoda-ku, Tokyo 101-8010<br>Japan |
| II-6 | 国籍（国名） | 日本国 JP |
| II-7 | 住所（国名） | 日本国 JP |
| III-1 | その他の出願人又は発明者 | |
| III-1-1 | この欄に記載した者は | 出願人及び発明者である (applicant and inventor) |
| III-1-2 | 右の指定国についての出願人である。 | 米国のみ (US only) |
| III-1-4ja | 氏名(姓名) | 桶屋 勝幸 |
| III-1-4en | Name (LAST, First) | OKEYA, Katsuyuki |
| III-1-5ja | あて名: | 244-0003 日本国<br>神奈川県 横浜市<br>戸塚区戸塚町5030番地<br>株式会社　日立製作所　ソフトウェア事業部内 |
| III-1-5en | Address: | c/o Software Division, HITACHI, LTD.<br>5030, Totsukacho, Totsuka-ku,<br>Yokohama-shi, Kanagawa 244-0003<br>Japan |
| III-1-6 | 国籍（国名） | 日本国 JP |
| III-1-7 | 住所（国名） | 日本国 JP |

| | | |
|---|---|---|
| IV-1 | 代理人又は共通の代表者、通知のあて名<br>下記の者は国際機関において右記のごとく出願人のために行動する。 | 代理人 (agent) |
| IV-1-1ja | 氏名(姓名) | 浅村 皓 |
| IV-1-1en | Name (LAST, First) | ASAMURA, Kiyoshi |
| IV-1-2ja | あて名: | 100-0004 日本国<br>東京都 千代田区<br>大手町２丁目２番１号　新大手町ビル３３１ |
| IV-1-2en | Address: | Room 331, New Ohtemachi Bldg., 2-1,<br>Ohtemachi 2-chome,<br>Chiyoda-ku, Tokyo 100-0004<br>Japan |
| IV-1-3 | 電話番号 | 03-3211-3651 |
| IV-1-4 | ファクシミリ番号 | 03-3246-1239 |
| IV-2 | その他の代理人 | 筆頭代理人と同じあて名を有する代理人<br>(additional agent(s) with same address as first named agent) |
| IV-2-1ja | 氏名 | 浅村 肇 |
| IV-2-1en | Name(s) | ASAMURA, Hajime |
| V | 国の指定 | |
| V-1 | 広域特許<br>(他の種類の保護又は取扱いを求める場合には括弧内に記載する。) | EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR<br>及びヨーロッパ特許条約と特許協力条約の締約国である他の国 |
| V-2 | 国内特許<br>(他の種類の保護又は取扱いを求める場合には括弧内に記載する。) | US |
| V-5 | 指定の確認の宣言<br>出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。 | |
| V-6 | 指定の確認から除かれる国 | なし (NONE) |
| VI-1 | 先の国内出願に基づく優先権主張 | |
| VI-1-1 | 出願日 | 2000年11月08日 (08.11.2000) |
| VI-1-2 | 出願番号 | 特願2000-345457 |
| VI-1-3 | 国名 | 日本国 JP |
| VI-2 | 先の国内出願に基づく優先権主張 | |
| VI-2-1 | 出願日 | 2000年12月21日 (21.12.2000) |
| VI-2-2 | 出願番号 | 特願2000-393279 |
| VI-2-3 | 国名 | 日本国 JP |

| | | | |
|---|---|---|---|
| VII-1 | 特定された国際調査機関(ISA) | 日本国特許庁 (ISA/JP) | |
| VIII | 申立て | 申立て数 | |
| VIII-1 | 発明者の特定に関する申立て | - | |
| VIII-2 | 出願し及び特許を与えられる国際出願日における出願人の資格に関する申立て | - | |
| VIII-3 | 先の出願の優先権を主張する国際出願日における出願人の資格に関する申立て | - | |
| VIII-4 | 発明者である旨の申立て（米国を指定国とする場合） | - | |
| VIII-5 | 不利にならない開示又は新規性喪失の例外に関する申立て | - | |
| IX | 照合欄 | 用紙の枚数 | 添付された電子データ |
| IX-1 | 願書（申立てを含む） | 4 | - |
| IX-2 | 明細書 | 156 | - |
| IX-3 | 請求の範囲 | 9 | - |
| IX-4 | 要約 | 1 | e6369-00.txt |
| IX-5 | 図面 | 45 | - |
| IX-7 | 合計 | 215 | |
| | 添付書類 | 添付 | 添付された電子データ |
| IX-8 | 手数料計算用紙 | ✓ | - |
| IX-17 | PCT-EASYディスク | - | フレキシブルディスク |
| IX-18 | その他 | 納付する手数料に相当する特許印紙を貼付した書面 | - |
| IX-19 | 要約書とともに提示する図の番号 | 2 | |
| IX-20 | 国際出願の使用言語名： | 日本語 | |
| X-1 | 提出者の記名押印 | | |
| X-1-1 | 氏名(姓名) | 浅村 皓 | |
| X-2 | 提出者の記名押印 | | |
| X-2-1 | 氏名(姓名) | 浅村 肇 | |

受理官庁記入欄

| | | |
|---|---|---|
| 10-1 | 国際出願として提出された書類の実際の受理の日 | |
| 10-2 | 図面： | |
| 10-2-1 | 受理された | |
| 10-2-2 | 不足図面がある | |
| 10-3 | 国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日） | |
| 10-4 | 特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日 | |
| 10-5 | 出願人により特定された国際調査機関 | ISA/JP |

| | | |
|---|---|---|
| 10-6 | 調査手数料未払いにつき、国際調査機関に調査用写しを送付していない | |

国際事務局記入欄

| | | |
|---|---|---|
| 11-1 | 記録原本の受理の日 | |